VineetThesisAyodhya.docx

By Munesh Trivedi

WORD COUNT	11330	TIME SUBMITTED	21-MAR-2021 05:19AM
		PAPER ID	70196429

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

DNA	**Deoxyribonucleic acid**
ICS	Indexed Based Chaotic Sequence
ICSECV	Indexed Chaotic Sequence based Selective Encryption of Compressed Video
ZDT	Zero Distortion Technique
LSB	Least Significant Bit Substitution
LM	Location Matrix
DES	Digital Encryption Standard
AES	Advanced Encryption Standard
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio

CONTENTS

ABSTRACT

In the internet world, some of the information exchange required services defined in the security services X.800. Confidentiality of sensitive data is considered to be one of the security service defined in X.800 which is highly desirable in digital world. Encoding the sensitive information with the help of secret keys helps in maintaining the confidentiality of data. This approach is known as cryptography. The major limitation of cryptographic approaches lies in the fact that the encoding message which was or were produced as output after encryption procedure may attract malicious user on communication channels. They may launch brute force attacks or practice cryptanalysis. This limitation of cryptographic approaches is taken care by steganographic approach. Through steganographic approach one can conceal secret information into carrier. Carrier may be text, audio, image or video. The major limitation of steganography lies in the fact that, if any how steganalyst may aware about the fact that something is concealing in the carrier then purpose of steganography is defeated. This presented thesis discusses about an approach which utilizes the potential of both i.e. cryptography concepts and steganography concepts. For performing encryption DNA encoding procedure has been used. For hiding purpose Kekre's Advanced Multiple least significant bits substitution algorithm has been used. Simulation results signify that presented approach has strength in terms of high payload capacity, robustness, visual detection and time.

Keywords:Steganography, Image, LSBs, Digital data, Encoding, Carrier medium, HTML steganography, zero distortion technique

INTRODUCTION

1. Introduction

In the era of twenty century which is also considered as digital era, it is difficult to imagine a world without internet. Every single information is now thought to be stored in digital format so that it is accessible throughout the world without the limitations of locations. But everything is access to everybody? Or some restrictions on information have been put. This is decided by the data owner. Creator may think that information should be public or may have some restrictions in access its contents. Information can be thought as an asset which needs confidentiality, integrity and its availability when it's needed [1-69]. Making information as public in broad terms means that it is available to everyone without any restrictions. Or one can think as public access as information access to everyone which does not cause any harm to its creators or any person in the world (ethics). Certain information which are available on internet may require AAA i.e. authentication, authorization and accounting. Here term authentication means that any user wants to access a particular kind of information, he/she needs to authenticate first with the help of suitable login credentials. Once user has been logged successfully he/she has been authorized to do certain kind of tasks. The third A means accounting which is used for accounting information in accessing network resources[1].

AAA concept which helps in network management and security requires some efficient algorithms which ensure its implementation. Information may require confidentiality depending on its nature not only during storage but also during its transmission from one host on a network to another host over the internet. Security attacks threaten confidentiality, integrity and availability. Snooping and traffic analysis is considered to be main threat to information confidentiality. ITU-T (X.800) defines the services related data confidentiality. The list of X.800 includes:

a) Authentication: Identification of claiming client

b) Access Control: How to prevent unauthorized uses of computer resources.

c) Confidentiality: Data remains disclosed to unauthorized user.

d) Data Integrity: Data was intact and it is in its original form as sent by its authorized sender.

e) Non-Repudiation: concept is, parties if it is involved in authorized communication may not deny later i.e. protection against denial.

In simple words one may think as function of security in terms of storage. In digital sense it may be storing information in encrypted form and only authorized user who has the key/key's, may access that secured encrypted information. This approach is termed as cryptography. Cryptography word was of Greek origin which means "secret writing". Terms which used in cryptography are as follows:

a) Plain text: The original message which required security i.e. confidentiality.

b) Cipher text: The encoded message which is obtained from plain text after some security algorithmic procedure.

c) Cipher: The security algorithmic procedure.

d) Key: The secret text in the form of numbers or text or combination of both which is used by cipher algorithm and known only to authorize communicating party.

e) Encipher: Encipher means process of converting plain text i.e. original message into cipher text i.e. encoded message.

f) Decipher: Decipher means process of converting encipher text i.e. encoded message into plain text i.e. original message.

g) Cryptography: The domain which involves study of developed and developing concepts of encryption.

h) Cryptanalysis: In simple words: code breaking. The domain which involves the extraction of original information from encoded or cipher message without being aware of key or keys.

i) Cryptology: The practice of studying both the concepts i.e. cryptography and cryptanalysis.

j) Cryptographers: The person who studies and performs cryptographic practices in order to secure the message i.e. secret text is known as cryptographers.

k) Cryptanalyst: in simple words, the person or security expert who practices the cryptanalysis is popularly known to be cryptanalyst.

In broad terms two type of cryptography are practiced:

1.1 Symmetric key cryptography:

When encryption and decryption were performed with the help of same key by the communicating parties.

1.2 Public key cryptography:

When encryption and decryption were performed with the help of pair of key's by the communicating parties.

Now a days it is practiced through three mechanism i.e. symmetric key cryptography, public key cryptography and hashing. Some popular approaches of symmetric key cryptography are: IDEA, SERPENT, RC6 and DES etc. Some popular approaches of asymmetric key cryptography are: RSA, SSH etc. Figure 1 shows some popular approaches of cryptography that were widely used [1].

One may choose any of these algorithm to secure information. Transmission of encryptedmessage may create suspect and draw attention of hackers which on the one hand can be thought as limitation of cryptography. For example in military communications, one may sniff the traffic over the communication network if it is public and can locate the source and destination. Also it may get the longitude and latitude and duration of communication. Small-small information when combined may results in revealing in very sensitive information to unauthorized user on network. Generally the hackers or unauthorized user practices cryptanalysis. The objective of hacker or malicious user may not only to recover the original message but also the key or keys involve in encryption procedure. The general approaches involved in cryptanalysis are: cryptanalytic and brute force attacks.

Some of the popular approaches which are used in cryptanalytic were: cipher text only, known plain text, chosen plain text, chosen cipher text, chosen text. These are the approaches were practiced by cryptanalysis depending upon the information which they have.

Steganography approach may help in overcoming this limitation. The word steganography is derived from Greek word meaning “covered writing” or “conceal writing”. Steganographic approach is hiding a message into some carrier message that presence of message remains invisible. History is full of facts which show the use of steganography. Chinese people use to send their secret war messages by writing it on thin silk clothes which was then swallowed by their messengers. Invisible inks were used for covered writing in Rome and Greece.

Similarly tattooed heads or messages on heads were covered by hairs; secret messages written on wooden tables were replaces by wax etc. History is full of such practices.

Even now in modern era it is practiced widely.

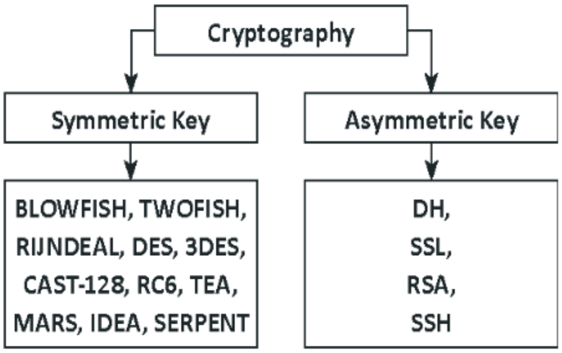

Cryptography
Symmetric Key
Asymmetric Key
BLOWFISH, TWOFISH, RIJNDEAL, DES, 3DES, CAST-128, RC6, TEA, MARS, IDEA, SERPENT
DH, SSL, RSA, SSH

Figure 1Cryptographic Classification[1]

One of such practice example is digital watermarking. Several media reports (Kelly [2001]) contains information [23] that natural images were used by terrorists for hiding their secret messages. Natural images were considered and are consider now a day's as carrier for hiding secret messages as natural images contains texture variations, contrasts and luminance.The steganographic practices were based on the key requirement that it does not degrade the quality of carrier image.

Concept is message should be as much as invisible.Idea is, it does not draw hacker attention. But if attacker/hacker comes to know about something hidden then he/she can uncover the information. Or even if attacker/hacker does not able to get the exact message but he/she suspect only, then also steganography purpose is defeated [25].

This fact can be considered as the major limitation of steganography. Covered writing should be performed in such a way that it should make very limited change in its carrier or carriers.

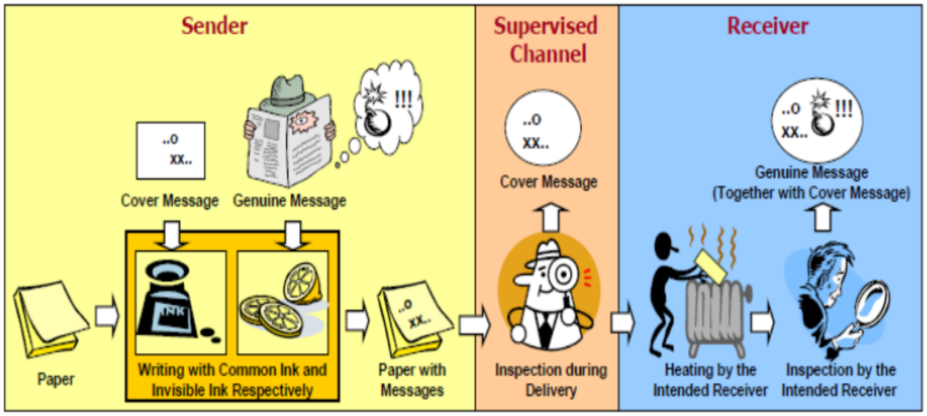

Sender
Supervised Channel
Receiver
..o xx..
Cover Message
Genuine Message
!!!
Paper
INK
Writing with Common Ink and Invisible Ink Respectively
Paper with Messages
..o xx..
Cover Message
Inspection during Delivery
..o xx.. !!!
Genuine Message (Together with Cover Message)
Heating by the Intended Receiver
Inspection by the Intended Receiver

Figure 2. A scenario using invisible ink [24]

Limited change will make steganalysis difficult. Some of the popular approaches in steganography were LSB, F3, F6 etc.

1.3 Issues Emerged (Gaps in Previous Studies/Research-Conceptual, Methodological and Theoretical) :

The past reviews of the literature of the research work done already shows that there is still ample scope on the topic of this research. There are some of the popular cryptographic approaches which are used now a day's [14-20].

Cryptosystem which was based on symmetric key has certain limitations which needs to be taken care:

- Exchange the secret key or keys
- Encryption and decryption procedure may involve number of keys
- Origin and authenticity of message guarantee etc.

Cryptosystem which was based on asymmetric key approach: there are certain issues involved which needs to be taken care:

- Authentication of public key
- Slow
- Need of computational resources during procedure etc.

But the major limitation of cryptographic approaches lies in the fact that its draws attention of malicious users. So to overcome this limitation, steganographic approaches can be used. Strength of steganographic approaches lies in the fact that it does not draw attention. But the limitation of steganographic approach lies in the fact that once the attacker comes to know that something is hidden inside the carrier then he/she may extract the secret message [3-21].

1.4 Motivation

Some of the researcher advocates to harness the potential of dual concepts i.e. steganography concepts and cryptography concepts [1-52]. Steganography and cryptography is considered to be orthogonal and complementary [25]. When both the concepts are used to hide the information, this is called metamorphic cryptography. The presented work is based on the concept of metamorphic cryptography.

Due to availability of high performing computational resources, launch of brute force attack can be performed in polynomial time, hence making traditional approaches strength questionable. This motivates security researcher to look for alternative approaches that can withstand with the emerging challenges. DNA can be thought as a strong alternative approach.

The main contribution of this work exploits the DNA approach for encrypting the text and KAMLA approach for performing the steganography. The potential of both the approaches has been utilized and a new approach was presented in the direction of performing metamorphic cryptography.

1.4 Organization Scheme:

Presented work was organized as follows:

Chapter I: Introduction

Chapter II: Detailed research work in this area.

Chapter III: Preliminary Studies

Chapter IV: Explains the problem definition and hypothesis

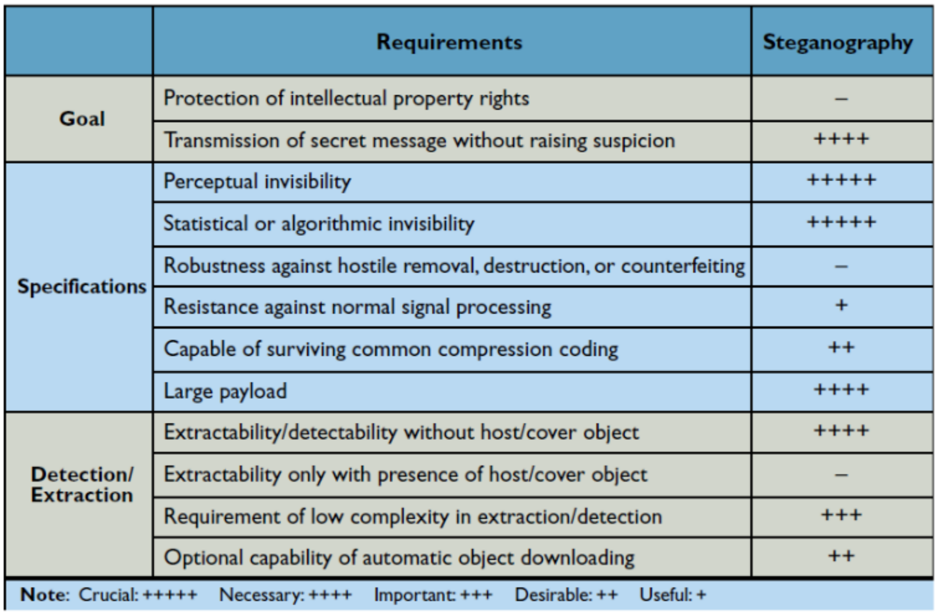
*Chapter V:*Explains the proposed methodology& proposed algorithm

Chapter VI: Result and Analysis

Chapter VII: Conclusion of the whole work presented in this thesis.

References and Appendices.

Table 1. Steganography: Goals, Specifications and Detection/Extraction [25]



	Requirements	Steganography
Goal	Protection of intellectual property rights	–
	Transmission of secret message without raising suspicion	++++
Specifications	Perceptual invisibility	+++++
	Statistical or algorithmic invisibility	+++++
	Robustness against hostile removal, destruction, or counterfeiting	–
	Resistance against normal signal processing	+
	Capable of surviving common compression coding	++
	Large payload	++++
Detection/ Extraction	Extractability/detectability without host/cover object	++++
	Extractability only with presence of host/cover object	–
	Requirement of low complexity in extraction/detection	+++
	Optional capability of automatic object downloading	++

Note: Crucial: +++++ Necessary: ++++ Important: +++ Desirable: ++ Useful: +

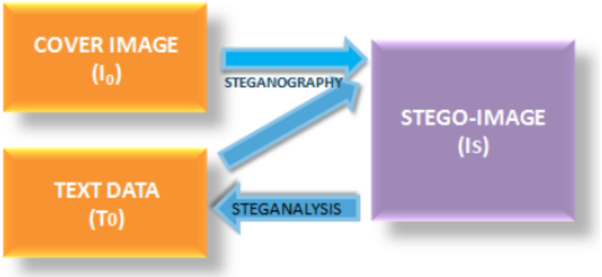


Figure 3.Schematic diagram of Steganography[2]

LITERATURE SURVEY

2. Literature Survey

This chapter describes the allied work in the domain of cryptography and steganography.

Authors in their work [3] presented a survey of traditional and modern approaches in cryptography such as RSA, RSA based singular cubic curve, JCE etc. They in their work also discuss some quantum cryptographic approaches such as RSA based on ECC with avk etc. Authors in their work [4] proposed metamorphic cryptography approach. For encrypting i.e. encoding the secret message, deoxyribonucleic (DNA) approach was used. Least significant approach was used to hide the message. Video was used as carrier medium to hide the encrypted text. Indexed based compression technique was used to compress the text. Authors in their work [5] presented video encryption procedure which was based on indexed chaotic sequence. They encoded I frame along with motion vector of video. Work [6] proposed a real time video encryption procedure namedICSECV. The ICSECV stands for indexed chaotic sequence based selective encryption of compressed video (ICSECV). They encoded the Intra coded frames from Group of pictures but in selective fashion. Chaotic theory was used by many security researcher because creates high amount of randomness to our input data. Randomness was added to create more confusion hence resulting in more secure output. As per researcher randomness and chaotic sequences can be think of synonyms of each other. Author in their research work [7] proposed metamorphic cryptographic approach using audio as carrier. For encrypting the text they had used indexed based chaotic sequence and for hiding purpose, LSB along with XOR approach has been used. It was hypothesized by the author that LSB along with XOR approach creates minimum distortion in the carrier. Authors in their work [8] supports the concept of metamorphic cryptography. Indexed based chaotic sequence was used for encryption and LSB was used for hiding purposes. As per authors, strength of using chaotic sequence is its randomness nature. LSB were used as it is very popular among its user for steganographic purposes. In simple words, it creates very less distortion in cover image. Author in their work [8] used video as carrier medium. Some authors used Zero Distortion Technique for hiding purposes [9]–[12]. One of the work [9] used ZDT approach for hiding purpose and index based chaotic sequence for encrypting text. Advantage of using ZDT approach as its name implies creates zeros distortion in cover image resulting in high PSNR values. Author in their proposed technique i.e. zero distortion technique, they matched common binary bits of secret data with binary bits of image pixels. The matched location was saved in another matrix. Author named this matrix as location matrix. This matrix contains location of matched binary bits of secret data with binary bits. The grey images were used as carrier image. These locations which are stored in location matrix were further encrypted to provide additional layer of security. For encrypting the locations in the location matrix they have used the concept of indexed based chaotic sequence. The location indexes in the location matrix were randomized by the indexes produced as output by the chaotic sequence formula.

$$X_{n+1}=\mu * X_n * (1-X_n) \qquad (1)$$

X_0 is an initial condition; value varies between 0 and 1. A control parameter μ value varies between 3.6 and 4.

The author in the presented work [10] used color images as carrier medium. The adding advantage of using color images was their three channels i.e. red blue and green. With the help of three channels, data can be concealed into any one of the three channels or all the three channels. Idea was use of three channels of color image increased the payload capacity i.e. more secret data can be concealed or hidden in cover image. The author in their work [10] first covert secret text into corresponding ASCII values. These ASCII values were further converted into binary values. Carrier image was chosen. In this work [10] carrier image was color image. The pixel values of this carrier image were extracted. These pixel values which were decimal values, converted into ASCII values. These ASCII values of pixels were further converted into corresponding binary values. The 8 bit binary values of text were matched with 8 bit binary values of cover image. The matched locations were saved into other matrix. This matrix was named as location matrix. This location matrix contains the locations where secret binary 8 bit values were matched with 8 bit binary values of cover image. This location matrix indexes were further jumbled. For jumbling these locations the author used concept of chaotic sequence. The equation one were the required formula which they have used to generate random indexes. With the help of random sequences the location matrix data were randomized. This location matrix was shared with receiver assuming that receiver has carrier image. Receiver on receiving this location matrix, applied chaotic sequence formula to generate the locations. Once the locations were obtained, receiver looked into carrier image to obtain the pixel values. The pixel values were converted into binary values. Finally the binary values were converted into ASCII values which further converted into corresponding letter resulting in secret text. If the secret text is large then three channels of image (color image) can be used for hiding intentions. Some researcher advocates the use of DNA based encryption and decryption [14] – [20], [28]. In paper [33], author presented concept of metamorphic cryptography. They encrypted their secret message with DNA concept. For hiding their secret message they have used least significant bit substitution approach. They [33] also used indexed based encryption technique for compressing their secret text.

The compression technique which was used was lossless compression technique. Authors [33] have used video as carrier medium. Video provides multiple frames options for hiding data. And if it is color video then it has three more channels which on the other hand provides three more options for hiding the secret data.

Authors [33] used indexed based chaotic sequence for selecting the frame of video in which secret text was hidden. Instead of using video frames sequentially for hiding the data, indexes are generated to create more confusion. Indexes were created with the help of equation- 1.

Chaotic sequence was generated with the help of formula as described in equation 1 above. Some researcher advocated the concept of bio-cryptography (DNA computers). In simple words, combining the concept of biology i.e. biometrics with cryptography. Biometric can be thought as science whose study involves understanding of evaluation of biological data. Biometrics were popular in the field of authentications. The biometric authenticate system use fingerprints, iris, face or combinations of these or physiological traits [33]. They can also use person speech or hand written system to authenticate. Idea was behavioral traits and physiological traits can be used as key with some other concept eliminating the need of long passwords or multiple passwords [32] [33]. They were also used in system which works in the domain of non-repudiation. The biometrics information were integrated with concept of cryptography in two popular ways [32] [33] i.e.

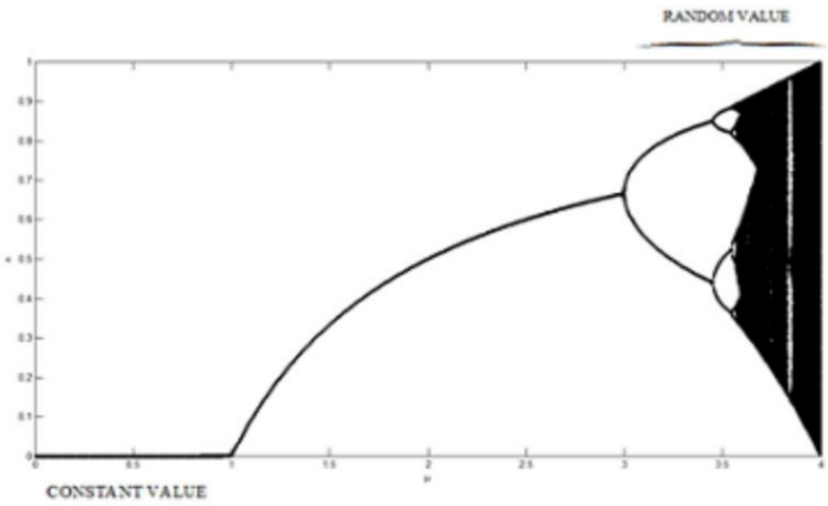


Figure 4. Logistic map: bifurcation diagram

2.1 Biometric based key release:

In biometric based key release approach, security system deploy a matching algorithm which tries to match a biometric signal which was input through devices with the data popularly known as template stored in database [32] [33]. If match is found successful then key is released otherwise it may ask of some number of attempts or retries.

2.2 Biometric based key generation:

In biometric-based key release approach keys were bounded (monotonically) to biometric signals [33].

The very adding advantage of biometrics over traditional practices is [32] [33]:

a) No need to remember

b) Guessing is difficult

c) No need to carry

d) No fear of stolen or loss

And it can be easily used in mixture with traditional approaches. Some researchers focused on the concept of DNA cryptography. DNA as it names implies, are long polymer which on other hand made up of millions of nucleotides which are linked together. Nucleotides contains a five carbon sugar, a phosphate group and one of nitrogen bases i.e. Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). The advantage of using DNA cryptography as mentioned in literature was [33]:

a) Speed: Very fast

b) Requirement of less or minimal storage: A compact volume can store large volume of data. As mentioned in literature, DNA one gram contains approximately 1021 DNA bases which on other hand can store 108 T B of data.

c) Less requirement of power

Pragya et al. in their paper presented [35] message authentication through steganography. Image was used as carrier medium. Idea was, hash of secret message was calculated using SHA- 1 algorithm. The hash code which was of 160 bits resulted as output of application of SHA-1 algorithm was converted to binary.

Carrier image was chosen. Pixels values of carrier image which were actually decimal values, converted into binary values. Least significant bit substitution method was chosen to hide the secret message. 160 bit hash code was hidden into LSBs of carrier image. If the LSB of pixel was same as binary value of hash, then there was no need to change in the LSB bit of carrier image, otherwise replace the LSB of carrier bit with message i.e. hash binary bit. This image after the LSB operation was saved and sends over the desired communication network to the designated recipient. There were some more tasks which were needed to perform at sender side as per presented paper. According to authors [35] they send hash of secret message after hiding it into carrier medium and secret message was encrypted with the encryption algorithm and this encrypted message was send over some other communication medium. For performing encryption they have used DES encryption algorithm. At the receiver end, the receiver decrypted the message following the reverse procedure of encryption algorithm. Receiver generated the hash code of decrypted message. The receiver used SHA-1 for calculating the hash of received message. On the other hand, receiver after receiving the stego image obtains the pixel values. These pixels values were in numeric form. These numeric numbers were converted into corresponding binary values. LSBs values were obtained. These LSBs binary values were converted into corresponding decimal values. And these decimal values were converted into corresponding character values. This step generated the hash message. This hash message which was received through carrier image was compared with the calculated hash of decrypted message. If they matched then it ensures that integrity of message was remaining intact. In simple worlds no change was made during transmission by any authorized user. If they didn't matched then it was concluded that message got altered. Author for generating hash of message used SHA-1 algorithm. They have given reasons why they have used SHA-1 over MD5. The reasons were as follows:

a) MD5 is more vulnerable to SHA-1.

b) Using MD5 has more chances of collision as compared to SHA-1. If hash is generated using MD 5 it will result in 128 bit message digest. And if hash is generated using SHA-1, it will result in 160 bit message digest (one in 2^{80}).

In 2004 MD 4 and MD 5 were proved to be more likely to have collisions. Many versions of SHA family were invented such as SHA-2. SHA-2 generated message digest were offered less collisions as compared to SHA-1. Several more versions of SHA families were SHA-256, SHA- 384, SHA- 512. SHA -256, SHA- 384, SHA -512 produces the hashes of messages which were of length 256, 384 and 512 respectively.

Author in their work [36] presented a metamorphic concept but using text as medium. Using text as medium has certain limitations such as: it is sensitive to changes, it lacks redundancy etc. In their work, input was secret text and carrier was also secret text. The sender side output was chaotic sequence matrix. The first step of sender side was to convert the cover text to corresponding ASCII values. These ASCII values were then converted into corresponding binary values. The secret text size was reduced. For reducing secret text size, they have used abbreviation method. The reduced secret text was converted into ASCII values. These ASCII values were converted into binary values [36]. The matching process was then performed. Matching was done between cover text and secret text. If match was found then location was recorded. These locations were saved in the location matrix. Chaotic sequence was then generated using the eq.- 1 as described above. Index was generated with the help chaotic sequence. Indexes were sorted. Location matrix was generated as output. Location matrix and cover text were then communicated into receiver side. On receiving the cover text, receiver extracted the matrix of locations. Convert the cover text file into corresponding ASCII values and then these ASCII values were converted into corresponding binary values. With the help of location matrix, binary values were obtained. These binary values were converted into ASCII values. These ASCII values were converted into corresponding letter. Output was secret text. Trivedi et. al. [37] in their work presented the combination of cryptography and steganography i.e. metamorphic approach. They have used audio as carrier medium. Secret text was chosen and carrier audio was chosen. The secret text was converted into corresponding ASCII values. These ASCII values of secret text were converted into corresponding binary values. Similarly the carrier audio was converted into corresponding ASCII values. These ASCII values were converted into binary values. Secret text was encrypted with the help of equation-1 as described. As per their considered example: secret text was “steganography”.

This word has 13 alphabets or letters. Corresponding ASCII values were: 115, 116, 101, 103, 97, 110, 111, 103, 114, 97, 112, 104, and 121. These ASCII values were converted into binary values. The paper [37] contains screen shots which show their step by step procedure. Consider first letter of secret text i.e. “s”. Its ASCII value is 115. Corresponding binary values were: 1 1 1 0 0 1 1. From equation 1 described above, they have generated the chaotic sequence matrix.

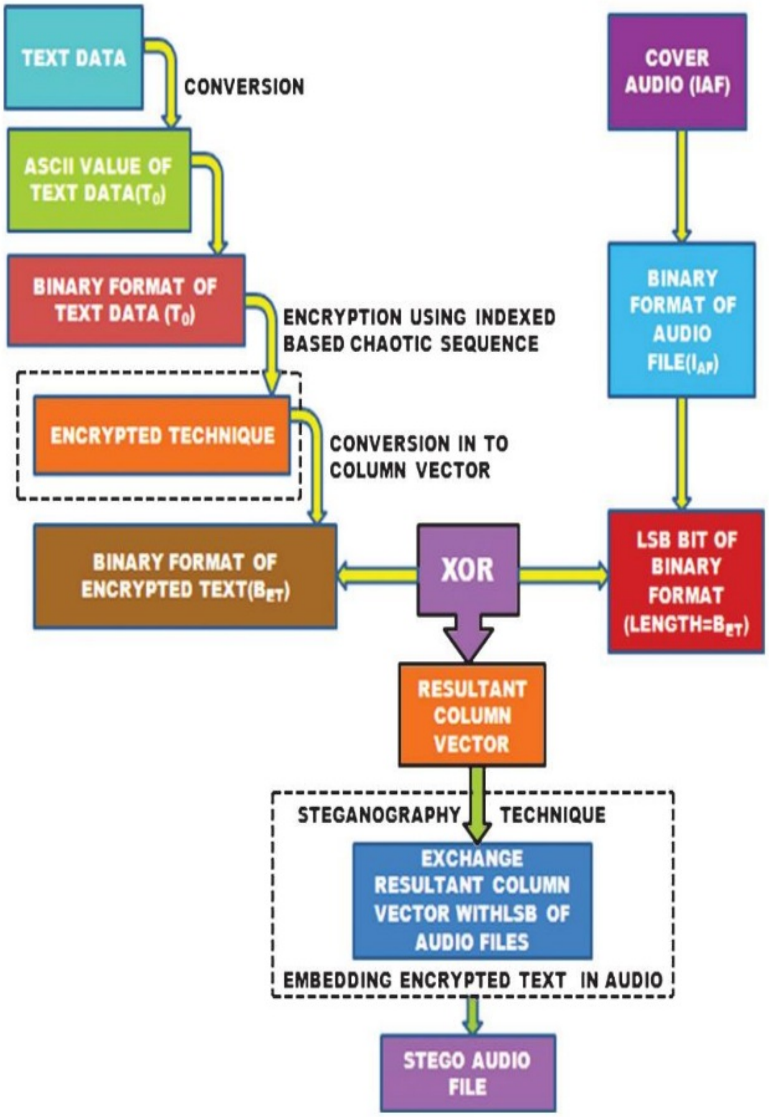

TEXT DATA
CONVERSION
ASCII VALUE OF TEXT DATA(T0)
BINARY FORMAT OF TEXT DATA (T0)
ENCRYPTION USING INDEXED BASED CHAOTIC SEQUENCE
ENCRYPTED TECHNIQUE
CONVERSION IN TO COLUMN VECTOR
BINARY FORMAT OF ENCRYPTED TEXT(BET)
XOR
COVER AUDIO (IAF)
BINARY FORMAT OF AUDIO FILE(IAF)
LSB BIT OF BINARY FORMAT (LENGTH=BET)
RESULTANT COLUMN VECTOR
STEGANOGRAPHY TECHNIQUE
EXCHANGE RESULTANT COLUMN VECTOR WITHLSB OF AUDIO FILES
EMBEDDING ENCRYPTED TEXT IN AUDIO
STEGO AUDIO FILE

Figure 5. Author proposed flow chart for performing embedding procedure [37]

As per their work, considered μ was equal to 3.62. X_0 were considered in the range of [0 1] i.e. 0.6. The next term generated with the help of chaotic formula was 0.6000. Similarly they have generated m x n terms matrix. Sort this m x n chaotic matrix. For example, the older location of 0.6000 was (1, 1) in chaotic matrix. The newer location after sorting matrix becomes (9, 6) (assume). Then secret text location after matching with cover text was embedded into this new location. This procedure was performed for all the characters of secret text. The resultant matrix after encryption procedure was converted into column vector or column matrix. Once this gets finished, steganography were performed. Audio file was chosen as cover. LSB of the cover audio file was also converted into column vector. The column vector obtained after encryption procedure was XORed with column vector of carrier audio file (i.e. LSBs of the carrier audio file). After XOR operation, the column vector which was resulted, were named as resultant column vector. This column vector i.e. resultant column vector replaced the LSBs of audio file. This resulted into stego audio file. This stego audio file was shared into the communication channel.

On the receiver side, reverse procedure was performed. The sender will share this stego file plus μ and X_0 value. Receiver on receiving this stego audio file converted this into corresponding binary values. LSBs from this carrier stego audio file were obtained (length equal to secret text message), say this as M_1. LSBs of the carrier image were also obtained, say this as M_2.Convert these two matrixes i.e. M_1 and M_2 into column vector. These two matrixes i.e. M_1 and M_2 were XORed. With the help of chaotic sequence the location of secret text were generated. This was done with the help of values of μ and X_0 shared with receiver by the sender. From these locations binary bits were obtained. A group of bits were formed.

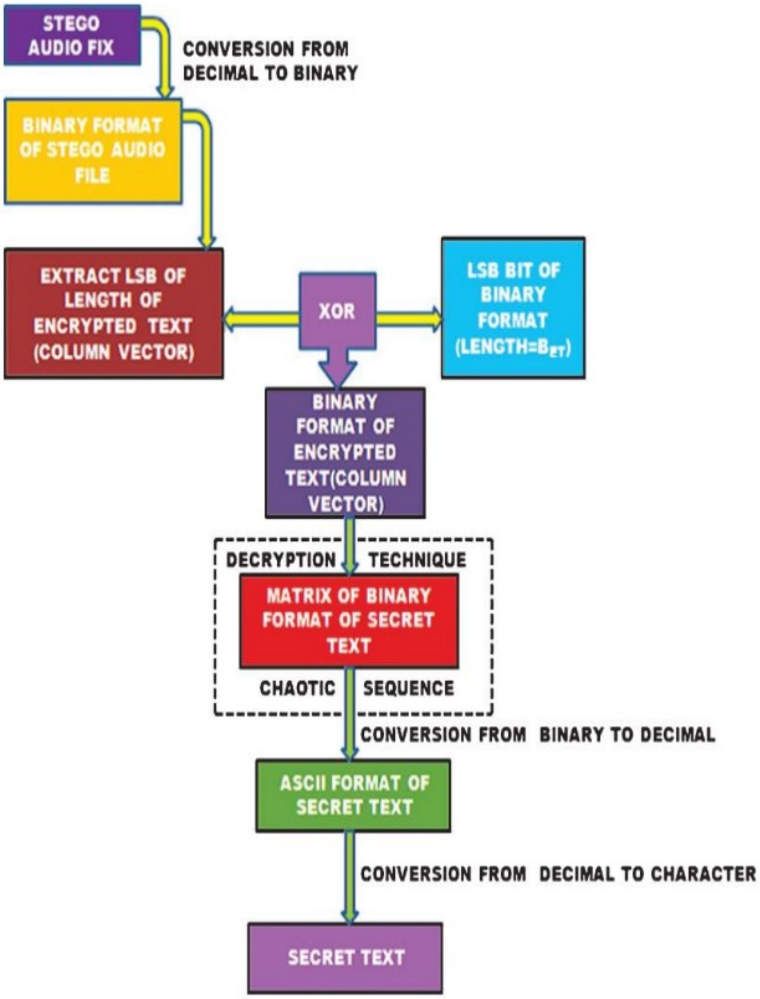

STEGO AUDIO FIX
CONVERSION FROM DECIMAL TO BINARY
BINARY FORMAT OF STEGO AUDIO FILE
EXTRACT LSB OF LENGTH OF ENCRYPTED TEXT (COLUMN VECTOR)
XOR
LSB BIT OF BINARY FORMAT (LENGTH=B$_{ET}$)
BINARY FORMAT OF ENCRYPTED TEXT(COLUMN VECTOR)
DECRYPTION TECHNIQUE
MATRIX OF BINARY FORMAT OF SECRET TEXT
CHAOTIC SEQUENCE
CONVERSION FROM BINARY TO DECIMAL
ASCII FORMAT OF SECRET TEXT
CONVERSION FROM DECIMAL TO CHARACTER
SECRET TEXT

Figure 6. Author proposed flow chart for performing decoding procedure at receiver side [37]

These groups were converted into corresponding ASCII values. These were the ASCII values of secret text. These texts were generated from these ASCII values. This was resulted in the secret text at receiver side. As per authors [37] their proposed work produces less distortion in the carrier audio file. AS per their claim, even human ears cannot suspect the audio distortion. LSB produces distortion, so the authors [37] along with LSBs, used XORed concept. Author in their research [38] paper presented other approach of metamorphic cryptography. For performing encryption they have used DES encryption algorithm. For performing steganography they have used LSB algorithm. DES symmetric cryptographic approach has been used. First secret text was encrypted with the help of DES encryption algorithm. This step resulted in cipher text. This cipher text was hidden using LSBs. Song et al. in their approach used the combination of LSB matching and Boolean functions in stream ciphers [39]. They used LSB for performing steganography. For performing encryption, they have used stream ciphers. Divya et al. in their proposed concept of metamorphic approach used RSA plus LSBs and MSBs concept. They have used RSA concept for encrypting their secret text. RSA was proved to very secure [40]. LSBs along with MSB were used for performing steganography. MSBs were also looked for hiding purposes. Idea was to create less distortion simultaneously increasing payload capacity of carrier image. In their proposed work they have used gray scale images. Author [41] in their presented work advocates the use of metamorphic cryptography. They [41] have encrypted the secret text using encryption algorithm. For hiding this secret text into carrier medium they have used LSBs substitution method. They have used audio files as carrier medium in which this secret text was hidden using LSBs approach after encryption. As per authors [41] their proposed approach were fit for any kind of audio format i.e. proposed approach can be used with any of the audio format. As it uses LSBs approach for hiding purposes which was very popular for creating very less distortion in carrier files. Authors in their paper [42] presented a concept which uses the dual key AES for encryption. One key was required at sender side for converting plain text into cipher text. Another key was required for converting cipher text into plain text. This key has to be shared in secure fashion. Sridevi et al. in their work [43] presented the concept of metamorphic cryptography but in reverse manner. They have proposed the concept: steganography followed by cryptography. Using LSBs approach they have hidden their plain text message. Once this step was performed successfully, they have used AES for encrypting whole stego image. AES stands for Advanced Encryption Standard. For hiding purposes they have used image files. Symmetric key encryption concept was used for encrypting the carrier stego image. This stego image was then shared over the internet or communication channel [43]. Receiver side after receiving this stego image decrypted using the same key which was shared by the sender through secure channel. After performing decryption, reverse procedure of LSBs was performed to obtain the secret text [43]. Authors in their work [44] presented the combination of angular encryption along with steganographic approach. They converted secret text into image i.e. cipher image. This cipher image was then hidden into another image. Receiver has to perform reverse steps to obtain the plain text.

Author et al. in their paper [45] presented a concept of video steganography. Authors have used video as carrier medium.

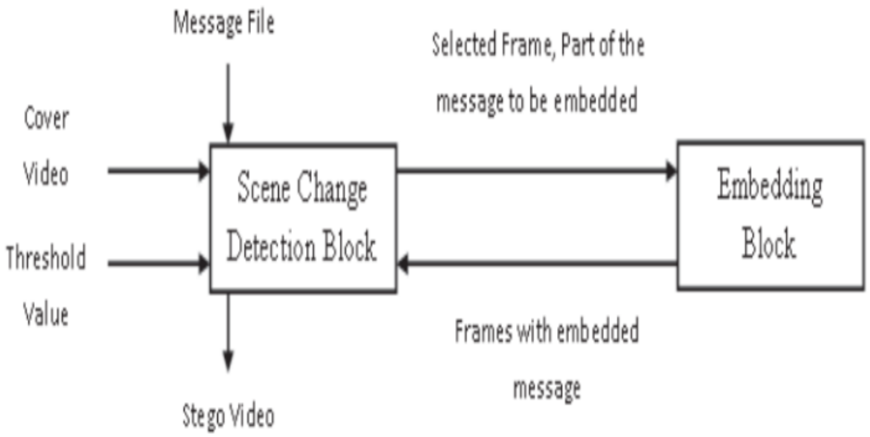

Message File
Selected Frame, Part of the message to be embedded
Cover Video
Threshold Value
Scene Change Detection Block
Embedding Block
Frames with embedded message
Stego Video

Figure 7. Schematic block diagram [45]

For hiding purposes they have used LSBs approach. The proposed concept was carried out in to two steps i.e. an embedding phase and decoding phase. Embedding phase consists of two steps i.e. scene change detection block and embedding block. Scene change detection block detects the scene changes. If there was scene change in the video frame, divided the messages into blocks. Histogram difference techniques were used to detect the scene change for a particular video frame. When abrupt changes were recorded by the scene change detection block, it sends the frame plus the message block to the next step i.e. embedding block. Embedding block followed the concepts of 3-3-2 approach. Authors have used LSBs concepts for hiding secret message. First secret message is converted into corresponding ASCII values. These ASCII values were converted into binary values. Similarly the corresponding frame which was selected, its pixels values were converted into corresponding ASCII values. These ASCII values were converted into corresponding binary values. As each frame in video contains three plane i.e. red, blue and green, a pixel were chosen from same locations. Three bits of secret message were hidden in three LSBs of red plane, next three bits of secret message were hidden in three LSBs of green plane and two bits of secret message were hidden in two LSBs of blue plane i.e. 3-3-2 approach. At the end they have added the NULL to indicate the end of secret message. Authors instead of directly embedding pixels into the video frame as send by scene change block, they have randomized the locations using the indexed based chaotic sequence concept [46]. They have also shown the result of MSE i.e. mean square error and PSNR i.e. peak signal to noise ratio. As per their results [45] they proposed concept resulted in low mean square error and high PSNR. As per authors the advantage of using change scene frame was to confuse the attacker that something was hidden into it.

In presented work DNA approach has used because it offers speed, minimum power and storage requirements [14]–[20], [33]. With the help of DNA approach the user can describe more complex encryption approach [20, 33]. The DNA encoding is performed using following steps [20]:

1. The message and key are converted into ASCII and then to binary values.

2. Padding of zeros are done if message or key size are not even.

3. XOR step 1 and Step 2

4. Output of step 3 is represented with the help of DNA bases format.

Decoding is performed in following steps:

1. Convert DNA formats to bits.

2. XOR the Step 1 and Key.

3. Convert the step 2 into binary and then ASCII code. Convert ASCII to character to get original message (plain text)

An explanation of implementation with an example was presented in proposed work section.

Authors in their work [2] presented a study which contains different methods of performing text steganography. For example methods based on semantic approach, open spaces or white space, format based etc. The most widely used steganography method was least significant bit substitution method. This method was popular in literature because of its easiness to implement. One desirable condition for LSB concept was that if compression were involved in process then it needs to be loss less. The reason was that, in LSB substitution, every LSB bit of pixel of cover image were involved. When 8-bit gray image were used, only one binary bit of secret text was embedded in only pixel of cover image. For example, suppose our text message is “Hello”. Convert this word to corresponding ASCII values and then to 8 bit corresponding binary values. Secret text message contains 5 X 8 = 40 bits which needs to be hidden in cover image. As per LSB approach for every bit, a pixel of cover image is needed. It means there is need of 40 pixels of the cover image. If carrier image was choosen as color image, then three bits of secret text can be hidden in carrier image. Color images have three channels i.e. red, blue and green (RGB), also known as 24-bit color image. So each pixels have three components i.e. red, blue and green. Using color images, payload capacity of carrier is increased. For example, suppose secret text first letter is ‘a’. The binary value of a is 0 1 0 0 0 0 0 1. To hide this 8 bits, only three pixels have to be used if carrier considered is color image. If gray image is considered as carrier then 8 pixels is needed. Consider a color image pixels has binary values: (0 0 0 0 0 0 0 0, 0 0 0 0 1 0 1 0, 0 0 0 0 1 0 0 0), (0 0 0 0 0 0 0 1, 0 0 0 0 1 0 0 0, 0 0 0 0 1 0 0 0), (0 0 1 0 0 0 0 0, 0 0 0 0 1 0 1 1, 0 0 0 0 1 0 1 1). Then after hiding first letter i.e. 'a' binary value 0 1 0 0 0 0 0 1 results in final values of cover pixels: (0 0 0 0 0 0 0 0, 0 0 0 0 1 0 1 1, 0 0 0 0 1 0 0 0), (0 0 0 0 0 0 0 0, 0 0 0 0 1 0 0 0, 0 0 0 0 1 0 0 0), (0 0 1 0 0 0 0 0, 0 0 0 0 1 0 1 1, 0 0 0 0 1 0 1 1) .

Authors in their work [13] proposed text steganographic approach based on LSB and indexed based chaotic sequence. Instead of applying LSB approach on whole frame, they applied where changes occur in consecutive frames. For creating randomness, pixels were jumbled with the help of chaotic sequence.

PRELIMINARY STUDIES

3. Preliminary Studies

For applying steganographic approach, KAMLA algorithm was used. KAMLA stands for Kekre's Advanced Multiple LSB algorithm [21]. KAMLA approach was an improvement over KIMLA approach [22]. As per author presented that KIMLA approach was an improvement over normal LSB substitution method. It increases the payload capacity of carrier image. Payload capacity was increase by 123% over LSB substitution method [22].

The same author [22] in their paper proposed KAMLA. KAMLA was again improvement over KIMLA. As per authors [22] KAMLA has more payload capacity than KIMLA approach. The KAMLA approach has improved the payload capacity by 146 % over traditional LSB substitution method. Strength of KAMLA and KIMLA approach is that instead of high payload capacity, maximum mean square error were found to be less than 4%. It means visual distortion of carrier or cover medium is very less, which makes detection difficult.

3.1 Kekre's improved Multiple LSB algorithm (KIMLA)

KIMLA stands for Kekre's Improved Multiple LSB algorithm. Table I and table II shows the Bit Replacement Concept (BRC) of KIMLA and KAMLA approach respectively.

3.2 Kekre's advanced Multiple LSB algorithm (KAMLA)

In proposed work KAMLA approach was used for hiding purposes. Strength of KAMLA approach is its payload capacity while creating less distortion in the cover image.

Table 2. Bit Replacement Concept KIMLA [22]

4MSB	**Decimal**	**Next Decimal**	**BRC**	**Changed Bits**
0000	Zero (0)	0001	One (1)	UUUC
0001	One (1)	0010	One (1)	UUUC
0010	Two (2)	0011	Two (2)	UUCC
0011	Three (3)	0100	One (1)	UUUC
0100	Four (4)	0101	Two (2)	UUCC
0101	Five (5)	0110	Two (2)	UUCC
0110	Six (6)	0111	Three (3)	UCCC
0111	Seven (7)	1000	One (1)	UUUC
1000	Eight (8)	1001	Two (2)	UUCC
1001	Nine (9)	1010	Two (2)	UUCC
1010	Ten (10)	1011	Three (3)	UCCC
1011	Eleven (11)	1100	Two (2)	UUCC
1100	Twelve (12)	1101	Three (3)	UCCC
1101	Thirteen (13)	1110	Three (3)	UCCC
1110	Fourteen (14)	1111	Four (4)	CCCC
1111	Fifteen (15)	1111	Four (4)	CCCC

In above table 2, U represents the unchanged bits in the cover image and C represents the changed bit in the carrier image or cover image.

Table 3. Bit Replacement Concept Kekre's Advanced Multiple LSB (KAMLA) [1]

4MSB	BRC	No of One's	Max BRC	Changed Bits (LSB)
0000	One (1)	Zero 0	One (1)	XXXC
0001	One (1)	One (1)	One (1)	XXXC
0010	Two (2)	One (1)	Two (2)	XXCC
0011	One (1)	Two (2)	Two (2)	XXCC
0100	Two (2)	One (1)	Two (2)	XXCC
0101	Two (2)	Two (2)	Two (2)	XXCC
0110	Three (3)	Two (2)	Three (3)	XCCC
0111	One (1)	Three (3)	Three (3)	XCCC
1000	Two (2)	One (1)	Two (2)	XXCC
1001	Two (2)	Two (2)	Two (2)	XXCC
1010	Three3	Two (2)	Three (3)	XCCC
1011	Two (2)	Three (3)	Three (3)	XCCC
1100	Three (3)	Two (2)	Three (3)	XCCC
1101	Three (3)	Three (3)	Three (3)	XCCC
1110	Four (4)	Three (3)	Four (4)	CCCC
1111	Four (4)	Four (4)	Four (4)	CCCC

In above table 3, X represents the unchanged bits in the cover image and C represents the changed bit in the carrier image or cover image.

PROBLEM DEFINITION

4. Problem Definition

Due to availability of high performing computational resources, launch of brute force attack can be performed in polynomial time, hence making traditional approaches strength questionable. This motivates security researcher to look for alternative approaches that can withstand with the emerging challenges. DNA can be thought as a strong alternative approach.

The main contribution of this work exploits the DNA approach for encrypting the text and KAMLA approach for performing the steganography. The potential of both the approaches has been utilized and a new approach was presented in the direction of performing metamorphic cryptography.

4.1 Objective of the Research:

The objective of proposed study is to harness the strength of both the approaches i.e. cryptography and steganography to enhance the confidentiality of secret message. The combination of cryptography and steganography is popularly known as metamorphic cryptography.

For encrypting the secret message DNA cryptography was used. Security researcher believe that DNA cryptography is hope for unbreakable encryption. DNA uses dual strand key i.e. one for encryption procedure and other for decryption procedure.

In proposed work KAMLA approach was used for hiding purposes. Strength of KAMLA approach is its payload capacity while creating less distortion in the cover image.

4.2 Hypothesis:

The presented hypothesis was based on the concept of metamorphic cryptography. For secret writing deoxyribonucleic (DNA) encoding was used and for covered writing Kekre's Advanced Multiple LSB algorithm (KAMLA) approach was used.

PROPOSED WORK

4 Proposed Work

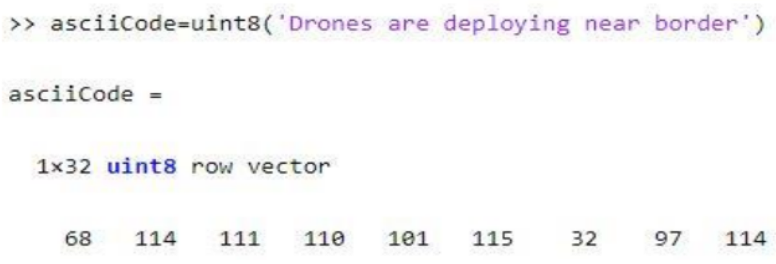
Proposed work is described in this chapter. Detailed of presented work is divided into two sub-sections i.e. encryption followed by hiding process and uncovers followed by decryption process.

5.1 Encryption followed by steganography

For performing encryption DNA approach have been used. To explain the proposed concept let's consider an example. Let say the message which needs security is:

"Drones are deploying near border"

Step1: Convert this message into ASCII bits. ASCII value of ' D ' is 68, similarly ' r ' is 114 etc. Figure 8 shows the MATLAB snippet containing ASCII values of considered message i.e. " Drones are deploying near border ".

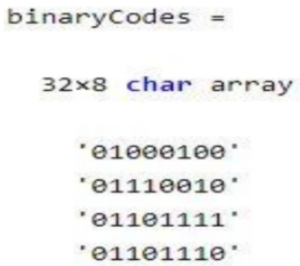


```
>> asciiCode=uint8('Drones are deploying near border')

asciiCode =

  1×32 uint8 row vector

    68   114   111   110   101   115    32    97   114
```

Figure 8. Snippet showing ASCII value of considered message.

Step2: Convert this message into respected binary values. Figure proclaims the MATLAB snippet of binary codes.

Step3: Check if zeros padding is required. Zeros padding is required in order to make size of binary codes even. The above consider message does not required zeros padding.



```
binaryCodes =

  32×8 char array

    '01000100'
    '01110010'
    '01101111'
    '01101110'
```

Figure 9. MATLAB Snippet showing some binary value of considered message.

Step4: The above procedure is repeated for the key also. Here it is assumed that transmitter (sender) and receiver have same secured key exchanged in secured fashion. Let’s say key is:

“code”

Step5: The message and keys binary values are XOR together. The XOR table is given below:

Table 4. XOR Table

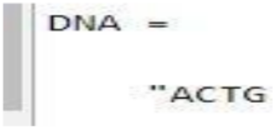
A	B	A XOR B

0	0	0
0	1	1
1	0	1
1	1	0

The XOR of first letter of the message i.e. D and key's first letter C is 0 0 1 0 0 1 1 1.

Step6: Once this process is completed for overall message with key, then DNA procedure is performed. A DNA strands is composite of mainly 4 nitrogenous bases i.e. Adenine (A), Thymine (T), Cytosine (C) and Guanine (G). The easiest way is to encode these four nitrogenous bases are: A- 0 0, T- 0 1, C- 1 0 and G- 1 1. Represent XOR output in DNA bases format i.e.

ACTG …



```
DNA =

      "ACTG
```

Figure 10. MATLAB Snippet showing DNA bases format of considered message.

To explain how DNA code ACGT was produced, consider a simple example. The first letter of secret text was "D" and the first letter of assumed secret key was 'c'. The decimal value of D is 68. The decimal value of 'c' is 99. The binary value of D i.e. 68 is 0 1 0 0 0 1 0 0 and the binary value of c i.e. 99 is 0 1 1 0 0 0 1 1. XOR of D i.e. 0 1 0 0 0 1 0 0 and c i.e. 0 1 1 0 0 0 1 1 is 0 0 1 0 0 1 1 1. The message which was obtained as result of XOR procedure was encoded with the help of DNA. Starting from left side of 0 0 1 0 0 1 1 1, 1 1 was represented by G, 0 1 was represented by T, 1 0 was represented by C and 0 0 was by A. So DNA encoding for the first letter of secret text i.e. was G T C A. Similarly this procedure was repeated for every letter of secret text resulting in encrypted text. One important thing was that in our case we have encoded the space also. Encryption process ends here.

Step7: After performing these steps successfully, KAMLA approach is applied to hide secret message in these DNA bases format. KAMLA is a spatial domain technique. Choose cover image i.e. carrier in which these DNA strands of secret message can be hidden. Here image was used as carrier medium. MATLAB inbuilt image "tire.tif" has been choosen. Its first pixel value is 6. Binary representation of decimal value 6 is 0 0 0 0 0 1 1 0. Select four MSB i.e. 0 0 0 0. Decimal value of choosen MSB is 0. Next decimal number to 0 is 1 and four bit binary representation of one is 0 0 0 1. As per KIMLA approach, from the Table I, BRC is one. It means only one bit can be replaced for four bit of LSB's i.e. X XX c. But KAMLA approach was used. Find out the sum of four MSBs i.e. 0 0 0 0. The sum of four MSBs is 0. So from Table II maximum BRC was found. This means count of bit replacement is 1. Maximum BRC is one. So only one bit of DNA output can be hidden in cover image i.e. X XX c. Encoded secret message was G T C A. The corresponding ASCII values for G T C A were 68 84 67 65. The binary value corresponding to 68, 84, 67 and 65 were: 0 1 0 0 0 0 0 1, 0 1 0 0 0 0 1 1, 0 1 0 1 0 1 0 0 and 0 1 0 0 0 1 0 0. This final bit stream 0 1 0 0 0 0 0 1 0 1

0 0 0 0 1 1 0 1 0 1 0 1 0 0 0 1 0 0 0 1 0 0 . . . were hidden in the cover image i.e. tire.tiff. Binary value of cover image i.e. carrier image was 0 0 0 0 0 1 1 0. First bit of final stream was 0. Only one bit of cover i.e. carrier image can be changed. So final value of first pixel of carrier image after embedding was 0 0 0 0 0 1 1 0. So it seems no change had been made for the first pixel. This process is repeated until all the binary values of DNA output step are made hidden.

5.2 Uncovering process followed by decryption

To obtain original message, reverse process have to be followed. Receiver side will receive stego image. Obtain binary values corresponding to decimal values of pixels in the image. For example, decimal value of first pixel of carrier stego image is 6. Binary equivalent to this is 0 0 0 0 0 1 1 0. Pick four MSB i.e. 0 0 0 0. Decimal equivalent to these MSB's are 0. Next decimal value to 0 is one. So BRC is one. Find out the max BRC. Sum of first four bits of MSBs are 0. So max BRC was 1. Hence only one message bit is hidden in this pixel. So obtain one message bit from LSB i.e. 0. Check next pixel. Repeat this procedure until all the hidden bits are uncovered from cover image. After uncovering all the hidden bits, obtain corresponding decimal values. Reverse process of DNA procedure is performed. For example, uncover bits are 0 0 1 0 0 1 1 1… Corresponding DNA coding: A C T G…

Convert this to binary values and XOR with key to obtain binary values of original message. Convert these binary values to decimal values which are nothing but ASCII values of characters of original message. Convert this ASCII values to corresponding letters.

5.1.1 Encryption followed by hiding (hiding(Encryption(Secret Message, Key), cover image))

1) Input message and key. Choose cover image. Convert message and key to respective ASCII values followed by respective binary values. Let's say these all binary values of message as b_1 and key as K_1.

2) xorBitWise=XOR (b_1, K_1)

3) Perform DNA encoding (ACGT / for example A=00; T=01 etc.) of step 2 output i.e. DNA (xorBitWise)

4) Select cover image.

5) Apply KAMLA concept to o/p of step 3 and step 4. i. e. KAMLA (S-3, S-4).

6) Output: stego image.

5.2.1Uncovering followed by Decryption (decryption (uncovering (Secret Message from image)), key)

1) Input: stego image (received at receiver side).

2) Implement reverse concept of KAMLA algorithm to obtain message.

3) Apply reverse concept of DNA algorithm.

4) Output of step 3 results original message.

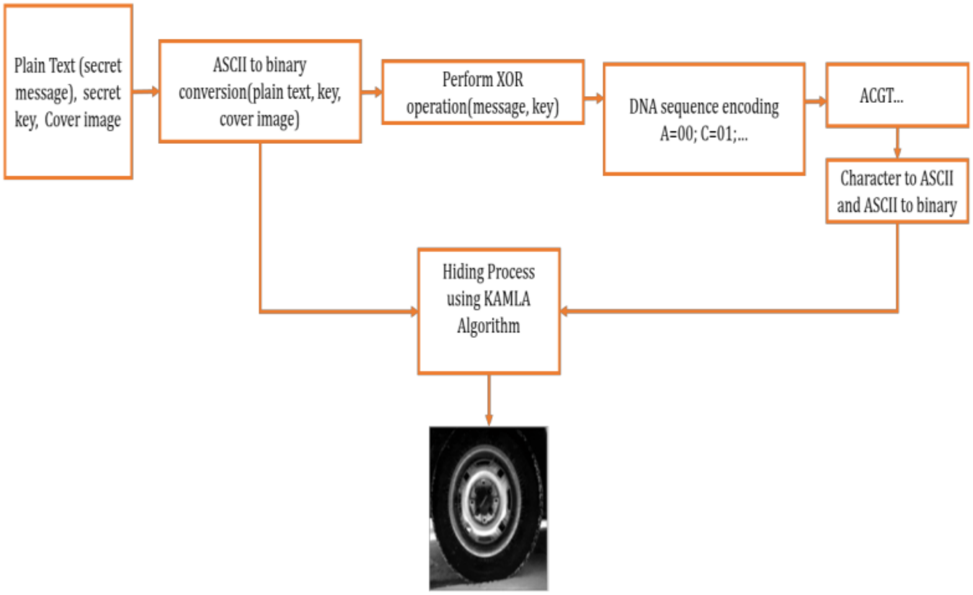

Plain Text (secret message), secret key, Cover image
ASCII to binary conversion(plain text, key, cover image)
Perform XOR operation(message, key)
DNA sequence encoding A=00; C=01;...
ACGT...
Character to ASCII and ASCII to binary
Hiding Process using KAMLA Algorithm

Figure 11. Figures shows the systematic diagramof proposed concept (encryption followed by hiding process)

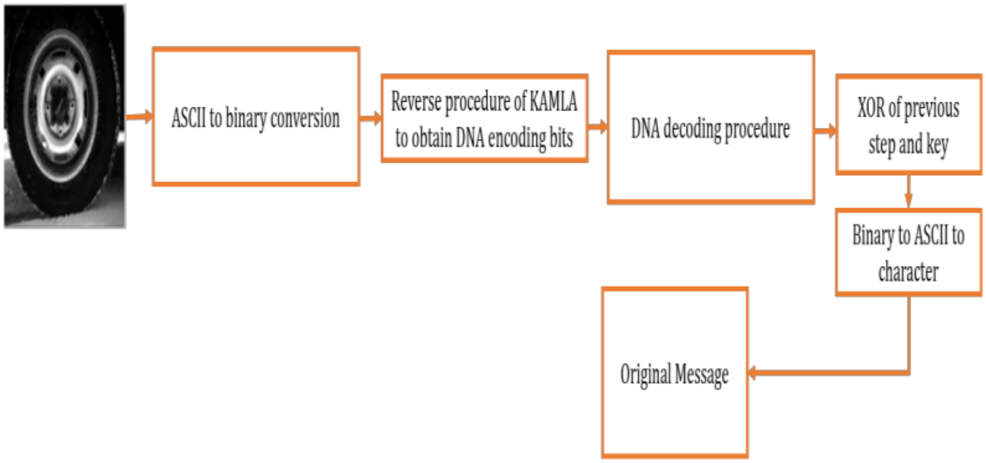

ASCII to binary conversion
Reverse procedure of KAMLA to obtain DNA encoding bits
DNA decoding procedure
XOR of previous step and key
Binary to ASCII to character
Original Message

Figure 12. Figure shows the systematic diagramof proposed concept (uncovering followed by decryption process)

RESULT & DISCUSSION

6. Result and Discussion

Table III shows the results of proposed approach on the basis of parameters. Proposed algorithm is robust as it uses DNA encryption. Proof of DNA encryption can be well found in available literature. The proposed algorithm uses KAMLA algorithm for cocealing secret message. KAMLA algorithm uses four LSB bits of carrier image for hiding purposes resulting in high payload capacity without creating distortion in carrier image. So it satisfies the performance on second parameter. Also using KAMLA approach for performing steganography creates less distortion in carrier image making visual detection difficult. Or if any steganalyst finds or suspect that carrier image contains some information then spectral analysis will result in encrytpted message. The proposed approach also satisfies the parameter of confusion as it uses DNA approach for encrypting message. Table III contains summary of the performance of proposed approach against parameters i.e. robustness, payload size, visual detection, steganalysis, confusion.

Table 5. LSB vs suggested approach (DNA+KAMLA) on Different specifications

Specifications	**Suggested Approach**
Robustness	Satisfactory due to DNA encryption approach
Payload Size	High due to KAMLA approach

Visual Detection	Very low due to less distortion created by KAMLA approach on cover image
Steganalysis	Spectral analysis may result in encoded message (potential)
Confusion	High due to DNA + XOR approach

Table 6 shows the implementation time means time taken by proposed approach in encryption and hiding process. Table VII also shows the time variation as per size of varying message length. The reason why time consumption is little higher than some of the proposed algorithm available in literature was due to DNA encoding procedure.

Table 6. Time consumption by proposed method while varying size of text message size (in bytes)

Carrier image	**Format**	**Dimensions**	**Secret text (in bytes)**	**Time (Suggested Algorithm)**
greens	.jpg	300 x 500	80	2.1
tire	.tif	205 x 232	120	2.3
circuit	.tif	280 x 272	512	7.3
plane	.png	256x256	648	7.8
pout	.tif	291x240	784	7.9

Image formats considered are png, tif, jpg etc. MatLab inbuilt images have been used because of their universal acceptance.

Figure no-9 contains carrier image, respective stego image and their histograms. Form images, it is straight forward that visual detection is hard. Histogram analysis shows very less disparity.

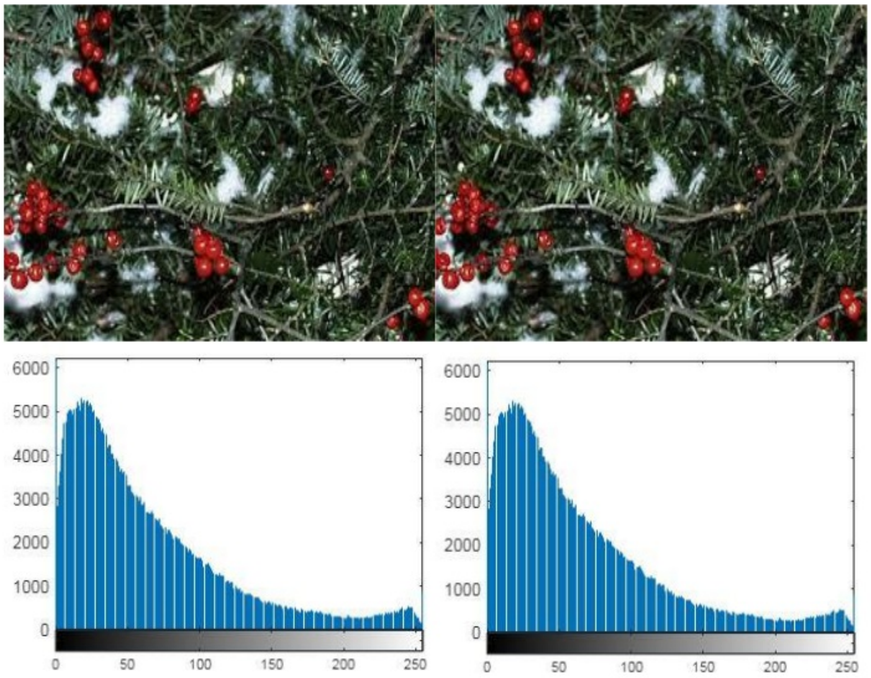


Figure 13. First four figures a) Original image (left) b) Stego Image(right) c) Histogram(left below) (original image) d) Histogram(right below) (stego image)

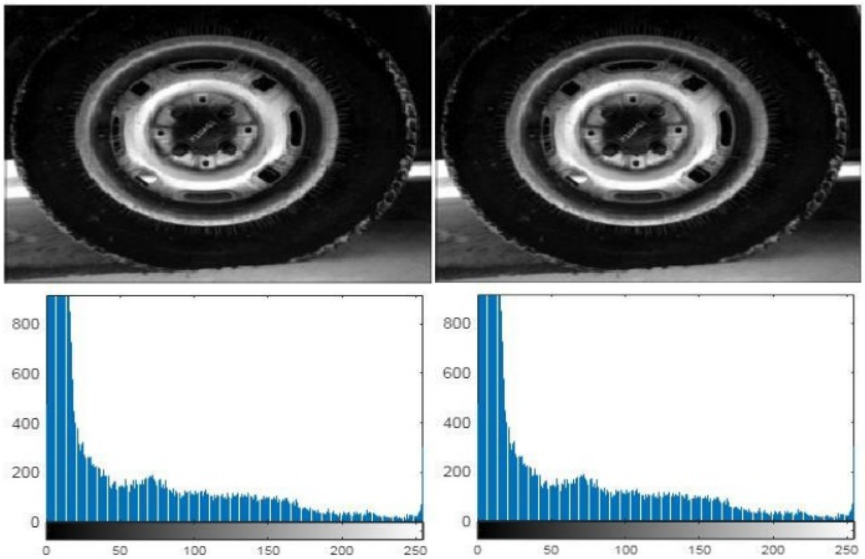


Figure 14. First four figures a) Original image (left) b) Stego Image(right) c) Histogram(left below) (original image) d) Histogram(right below) (stego image)

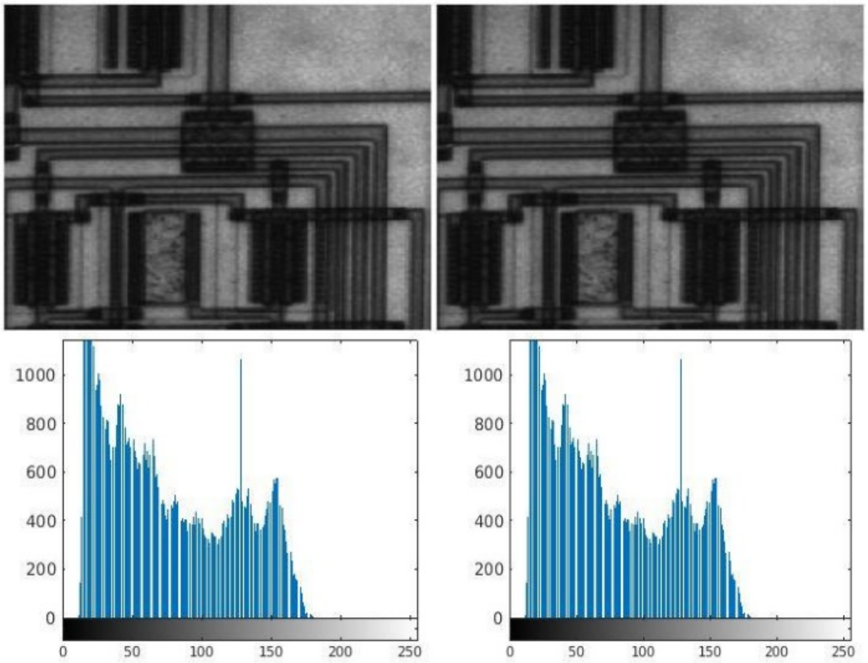


Figure 15. First four figures a) Original image (left) b) Stego Image(right) c) Histogram(left below) (original image) d) Histogram(right below) (stego image)

CONCLUSION

7. Conclusion

Fool proof information security system is need of today's digital world. Two approaches i.e. cryptography and steganography were followed inorder to secure information. Using combination of both the concept is popularly known as metamorphic cryptography in literature. Strength of cryptography inherit in the fact that secret message was converted into encoded form which is of no use until secure key is known. The strength of steganography lies in the fact that it does not attract anybody attention. If only cryptographic approach was used to secure the digital information, it may draw the attention of network sniffers or cryptanalyst. These sniffers or cryptanalyst may launch the brute force attack or some other attacks to obtain the encryption key or keys or secret text. Whereas, on the other hand if steganography was the only used concept for providing security to secret text, then it may not draw the attention. But steganalyst, if anyhow comes to know or even suspects that something was hidden inside carrier medium, then purpose of steganography fails. It is highly recommended by the security researcher to use both the concepts i.e. cryptography and steganography to provide security to digital secret text. Potential of both steganography concepts and cryptography concepts through KAMLA and DNA algorithms have been used in proposed work. The use of DNA encoding in message encryption has been proposed by several researcher and can be found in available literature. DNA approach is quiet popular in literature in terms of robustness, strongness and efficiency and thought to be unbreakable. The use of KAMLA approach which was used to implement steganographic concept, was an improvement over KIMLA and traditional LSB approaches. With the help of KAMLA approach payload capacity of message hiding in cover image has been increased in comparison to several LSB based approaches. Use of KAMLA approach for hiding purposes make visual steganalysis difficult as it produces less distortion in carrier image simultaneously increasing the payload capacity. Implementation was done on MATLAB 2020a and MATLAB inbuilt images were used for validation of proposed concept. It was observed with the help of validation images that proposed concept was efficient when evaluated in terms of payload capacity, security, robustness etc. In future work different carriers medium and different versions of DNA can be implemented to enhance the payload and security.

REFERENCES

REFERENCES

References

[1] "Varaždin, Croatia zoran. hercigonja Zoran Hercigonja Druga gimnazija. 'Comparative Analysis of Cryptographic Algorithms.' (2017). at DuckDuckGo." [Online]. Available: https://duckduckgo.com/?t=ffab&q=%5B1%5D%09Varaždin%2C+Croatia+zoran.+hercigonja+Zoran+Hercigonja+Druga+gimnazija.+"Comparative+Analysis+of+Cryptographic+Algorithms."+(2017).&atb=v182-1&ia=web. [Accessed: 27-Jul-2020].

[2] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," in Proceedings - 2016 2nd International Conference on Computational Intelligence and Communication Technology, CICT 2016, 2016, pp. 130–133.

[3] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, "Traditional and Hybrid Encryption Techniques: A Survey," Springer, Singapore, 2018, pp. 239–248.

[4] V. K. S. Pooja Dixit, Munesh Chandra Trivedi, Avdhesh Kumar Gupta, Virendra Kumar Yadav, "Video Steganography using Concept of DNA Sequence and Index Compression Technique," Int. J. Eng. Adv. Technol., vol. 8, no. 5, 2019.

[5] S. Batham, A. K. Acharya, V. K. Yadav, and R. Paul, "A new video encryption algorithm based on indexed based chaotic sequence," in IET Conference Publications, 2013, vol. 2013, no. 647 CP, pp. 139–143.

[6] S. Batham, V. K. Yadav, and A. K. Mallik, "ICSECV: An efficient approach of video encryption," in 2014 7th International Conference on Contemporary Computing, IC3 2014, 2014, pp. 425–430.

[7] M. C. Trivedi, S. Mishra, and V. K. Yadav, "Metamorphic cryptography using strength of chaotic sequence and XORing method," J. Intell. Fuzzy Syst., vol. 32, no. 5, pp. 3365–3375, Jan. 2017.

[8] N. Singh, M. C. Trivedi, V. K. Yadav, and V. K. Singh, “Metamorphic cryptography considering concept of XOR and chaotic sequence: Using video as medium,” in 2017 9th International Conference on Information Technology and Electrical Engineering, ICITEE 2017, 2017, vol. 2018-Janua, pp. 1–6.

[9] S. Sharma, V. K. Yadav, and S. Batham, “Zero distortion technique: An approach to image steganography using strength of indexed based chaotic sequence,” in Communications in Computer and Information Science, 2014, vol. 467, pp. 407–416.

[10] Shivani, V. K. Yadav, and S. Batham, “Zero Distortion technique: An approach to image Steganography on color images using strength of chaotic sequence,” in ACM International Conference Proceeding Series, 2014, vol. 11-16-Nove, pp. 1–8.

[11] N. Singh and V. Kumar Yadav, “Trends in Digital Video Steganography: A Survey,” 2017.

[12] S. Sharma, V. K. Yadav, M. C. Trivedi, and A. Gupta, “Audio Steganography using ZDT: Encryption using indexed based chaotic sequence,” in ACM International Conference Proceeding Series, 2016, vol. 04-05-Marc, pp. 1–5.

[13] R. Paul, A. K. Acharya, V. K. Yadav, and S. Batham, “Hiding large amount of data using a new approach of video steganography,” in IET Conference Publications, 2013, vol. 2013, no. 647 CP, pp. 337–343.

[14] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, “A novel DNA computing based encryption and decryption algorithm,” in Procedia Computer Science, 2015, vol. 46, pp. 463–475.

[15] S. Vajjiravelu and A. Punitha, “A Novel Approach to an Algorithm for Voice Encryption using DNA based Cryptography.”

[16] M. Sabry, M. Hashem, and T. Nazmy, “Three Reversible Data Encoding Algorithms based on DNA and Amino Acids’ Structure,” 2012.

[17] H. M. Bahig and D. I. Nassr, “DNA-Based AES with Silent Mutations,” Arab. J. Sci. Eng., vol. 44, no. 4, pp. 3389–3403, Apr. 2019.

[18] H. Shaw, “A Cryptographic System Based upon the Principles of Gene Expression,” Cryptography, vol. 1, no. 3, p. 21, Nov. 2017.

[19] Monika and S. Upadhyaya, “Secure Communication Using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks,” in Procedia Computer Science, 2015, vol. 70, pp. 808–813.

[20] “DNA Cryptography - GeeksforGeeks.” [Online]. Available: https://www.geeksforgeeks.org/dna-cryptography/. [Accessed: 28-Jul-2020].

[21] H. B. Kekre, A. A. Athawale, and U. A. Athawale, “Increased cover capacity using advanced multiple LSB algorithms,” in International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011 - Conference Proceedings, 2011, pp. 25–31.

[22] “(PDF) Increased Capacity of Information Hiding in LSB’s Method for Text and Image.” [Online]. Available: https://www.researchgate.net/publication/242600389_Increased_Capacity_of_Information_Hiding_in_LSB’s_Method_for_Text_and_Image. [Accessed: 29-Jul-2020].

[23] Watters, P., Martin, F., and Stripf, H. S. 2008. Visual detection of LSB-encoded natural imagesteganography. ACM Trans. Appl. Percpt. 4, 1, Article 5 (January 2008), 12 pages. DOI = 10.1145/1328775 http://doi.acm.org/10.1145.1328775

[24] Chun-Hsiang et al. "Digital Invisible Ink and its Applications in Steganography". M&Sec'06, September 26–27, 2006, Geneva, Switzerland.Copyright 2006 ACM 1-59593-493-6/06/0009.

[25] Huaiquing Wang and Shuozhong Wank. "Cyber Warfare: Steganography vs Steganalysis". In Communications of the ACM, Vol. 47, No - 10.

[26]Lecture slides by Lawrie Brown for “Cryptography and Network Security”, 4/e, by WilliamStallings, Chapter 2 – “Classical Encryption Techniques”.

[27] W. Bender, N. Morimoto, A. Lu.”Techniques for data hiding”.IBM Syst.

J. 35 (3/4) (1996)313–336.

[28] G. Viji and J. Balamurugan.”LSB Steganography in Color and Grayscale Images without using the Transformation”. Bonfring International Journal of Advances in Image Processing,Vol. 1, Special Issue, December 2011.

[29] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. “Information
Hiding – A Survey”.Proceedings of the IEEE, special issue on protection of multimedia content, pp. 1062-1078, July 1999.

[30] Morkel.T, J.H.P. Eloff, M.S. Olivier.“ An Overview of Image Steganography ”.Proceedings of the Fifth Annual Information Security South Africa Conference ,Sandton, South Africa 2005.

[31] William Stalling, Cryptography and network security: Principles and Practices (4th edition), Prentice 2006, ISBN – 978 – 81 – 775 – 8774-6

[32] "Advanced Encryption Standard "(AES), National Institute of Standards and Technology (NIST), U.S. FIPS PUB 197 (FIPS 197),2001.

[33] Chandra Trivedi, M., Kumar Gupta, A., Kumar Yadav, V., & Kumar Singh, V. (2019). Video Steganography using Concept of DNA Sequence and Index Compression Technique. International Journal of Engineering and Advanced Technology (IJEAT), 8(5), 32–42. https://www.ijeat.org/wp-content/uploads/papers/v8i5/D6368048419.pdf.

[34] M. Freire-Santosa, J. Fierrez-Aguilara, J. Ortega-Garciaa “Biometric Technologies for Human Identification III, Proceedings of SPIE, Vol. 6202"

[35] Pragya Agarwal, Shilpi Gupta, AnuMehra. “Hybrid Web-page Segmentation and Block Extraction for Small Screen Terminals”. Published in proceedings of 4th International IT Summit Confluence 2013 - The Next Generation Information Technology Summit. Published by International Journal of Computer Applications (0975 – 8887).

[36] Shivani,Virendra Kumar Yadav, Saumya Batham. “A Novel Approach of Bulk Data Hiding using Text Steganography”. Published in proceedings of 3rd International Conference on Recent Trends in Computing 2015

(ICRTC-2015), Procedia Computer Science 57 (2015) 1401 – 1410.

[37] Trivedi, M., Mishra, S., & Yadav, V. (2017, January 01). Metamorphic cryptography using strength of chaotic sequence and XORing method. Retrieved October 09, 2020, from https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs169277.

[38] Dhawal Seth, L. Ramanathan,"SecurityEnhancement:Combining Cryptography and Steganography",International Journal of Computer Applications (0975 –8887) Volume 9– No.11, November 2010.

[39] Shouchao Song, JieZhangb,XinLiao,Jiao Du QiaoyanWen, "A Novel Secure CommunicationProtocolCombining Steganography and Cryptography", 2011. Published by Elsevier Ltd.Selection and/or peerunderresponsibility of [CEIS 2011]. In Advanced inControl EngineeringandInformation Science.

[40] S.S. Divya, M. Ram Mohan Reddy, " Hiding Text inAudio Using Multiple LSB Steganography And ProvideSecurity Using Cryptography" International journal OfScientific & Technology Reseaech Volume 1,Issue 6,July2012, ISSN 2277-8616 68 IJSTR©2012 www.ijstr.org.

[41] AbikoyeOluwakemiC,AdewoleKayodeS,OladipupoAyotunde J."
Efficient Data Hiding System usingCryptography and Steganography"
InternationalJournal of Applied InformationSystems (IJAIS) –ISSN: 2249-0868 Foundation of Computer Science FCS,New York, USA
Volume 4– No.11, December 2012– www.ijais.org.

[42] Yohan Suryanto,NurHayati,Hendra,Kusumawardhana,Dr. RiriFitri Sari," Dual Key triple Encryption TextBased Message Suing Cryptography & Steganography". Int.J.Computer Technology &Applications,Vol 4 (1),43-50 IJCTA | Jan-Feb 2013 Available. online@www.ijcta.com 43 ISSN: 2229-6093.

[43] Dr.R.Sridevi,Vijaya, Paruchuri,,K.S.SadaShiva Rao,“Image Steganography combined with Cryptography“,Council for Innovative Research Peer ReviewResearch Publishing System Journal: IJCT Vol 9, No 1,ISSN 22773061 976 | Page July 15, 2013editor@cirworld.com,www.cirworld.com,member.cirworld.com.

[44] Thomas LeontinPhiljon. , Venkateshvara Rao.“Metamorphic Cryptography - A Paradox betweenCryptography and Steganography Using DynamicEncryption”,IEEE-International Conference on RecentTrends in Information Technology, ICRTIT 2011 978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, AnnaUniversity, Chennai. June 3-5, 2011.

[45] R. Paul, A. K. Acharya, V. K. Yadav and S. Batham, "Hiding large amount of data using a new approach of video steganography," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 337-343, doi: 10.1049/cp.2013.2338.

[46] AradhanaSoni and Anuja Kumar Acharya, “A novel image encryption approach using an Index based chaos and DNA Encoding and its Performance Analysis,” International Journal of Computer Applications, Volume 47– No.23, June 2012.

[47] Mohamed Elsadig, Miss Laiha Mat Kiah, Bilal BahaaZaidan and Aos Alaa Zaidan, “High rate video streaming steganography,” Proceedings of the 2009 IEEE International Conference on Future Computer and Communication, 2009, pp. 672 – 675.

[48] Mishra S., Yadav V.K., Trivedi M.C., Shrimali T. (2018) Audio Steganography Techniques: A Survey. In: Bhatia S., Mishra K., Tiwari S., Singh V. (eds) Advances in Computer and Computational Sciences. Advances in Intelligent Systems and Computing, vol 554. Springer, Singapore. https://doi.org/10.1007/978-981-10-3773-3_56

[49] Namrata Singh and Virendra Kumar Yadav. Trends in Digital Video Steganography: A Survey. International Journal of Computer Applications 169(7):6-18, July 2017.

[50] S. Batham, V. K. Yadav and A. K. Mallik, "ICSECV: An efficient approach of video encryption," 2014 Seventh International Conference on Contemporary Computing (IC3), Noida, 2014, pp. 425-430, doi: 10.1109/IC3.2014.6897211.

[51] Aqeel I., Suleman M.B. (2019) A Survey on Digital Image Steganography Approaches. In: Bajwa I., Kamareddine F., Costa A. (eds) Intelligent Technologies and Applications. INTAP 2018. Communications in Computer and Information Science, vol 932. Springer, Singapore. https://doi.org/10.1007/978-981-13-6052-7_66.

[52] Swain, G.: Digital image steganography using variable length group of bits substitution. Proc. Comput. Sci. 85, 31–38 (2016).

[53] S. Namasudra, “Fast and secure data accessing by using DNA computing for the cloud environment”, IEEE Transactions on Services Computing. DOI: 10.1109/TSC.2020.3046471

[54] S. Namasudra, S. Sharma, G. C. Deka and P. Lorenz, “DNA computing and table based data accessing in the cloud environment”, Journal of Network and Computer Applications, vol.172, 2020. DOI: https://doi.org/10.1016/j.jnca.2020.102835.

[55] S. Namasudra and G. C. Deka, “Applications of blockchain in healthcare”, Springer, 2021. DOI: 10.1007/978-981-15-9547-9.

[56] S. Namasudra, “An improved attribute-based encryption technique towards the data security in cloud computing”, Concurrency and Computation: Practice and Exercise, vol. 31, no. 3, 2019. DOI: 10.1002/cpe.4364.

[57] S. Namasudra, D. Devi, S. Choudhary, R. Patan and S. Kallam, “Security, privacy, trust, and anonymity”, in Advances of DNA Computing in Cryptography, S. Namasudra and G. C. Deka, Eds., Taylor & Francis, pp. 138-150, 2018.

[58] S. Namasudra, R. Chakraborty, A. Majumder and N. R. Moparthi, “Securing multimedia byusing DNA based encryption in the cloud computing environment”, ACM Transactions onMultimedia Computing,

Communications, and Applications, vol. 16, no. 3s, 2020. DOI: https://doi.org/10.1145/3392665.

[59] S. Namasudra, G. C. Deka and R. Bali, “Applications and future trends of DNA computing”, in Advances of DNA Computing in Cryptography, S. Namasudra and G. C. Deka, Eds., Taylor & Francis, pp. 181-192, 2018.

[60] S. Namasudra, R. Chakraborty, S. Kadry, G. Manogaran and B. S. Rawal, “FAST: Fast accessing scheme for data transmission in cloud computing”, Peer-to-Peer Networking and Applications, 2020. DOI: 10.1007/s12083-020-00959-6.

[61] S. Namasudra, “Data access control in the cloud computing environment for bioinformatics”, International Journal of Applied Research in Bioinformatics (IJARB), vol. 11, no. 1, pp. 40-50, 2020.

[62] P. Pavithran, S. Mathew, S. Namasudra and P. Lorenz, “A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine”, Computers & Security. DOI: https://doi.org/10.1016/j.cose.2020.102160

REFERENCES

PUBLICATIONS

APPENDIX

VineetThesisAyodhya.docx

ORIGINALITY REPORT

7%

SIMILARITY INDEX

PRIMARY SOURCES

1	Vikash Yadav, Indresh Kumar Gupta. "A hybrid approach to metamorphic cryptography using KIMLA and DNA concept", International Journal of Computational Systems Engineering, 2019 Crossref	79 words — 1%
2	docs9.chomikuj.pl Internet	75 words — 1%
3	Anil Kumar, M. K. Ghose. "Overview of Information Security Using Genetic Algorithm and Chaos", Information Security Journal: A Global Perspective, 2009 Crossref	50 words — 1%
4	pnrsolution.org Internet	46 words — < 1%
5	J. K. Mandal, Arindam Sarkar. "An Adaptive Neural Network guided Random Block Length based Cryptosystem for online wireless communication (ANNRBLC)", 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 Crossref	33 words — < 1%
6	www.ijeat.org Internet	31 words — < 1%
7	www.geeksforgeeks.org Internet	29 words — < 1%
8	ijcsn.org Internet	23 words — < 1%

9	Acharya, A.K., R. Paul, S. Batham, and V.K. Yadav. "Hiding large amount of data using a new approach of video steganography", Confluence 2013 The Next Generation Information Technology Summit (4th International Conference), 2013. Crossref	22 words — < 1%
10	Ranjana Joshi, Munesh C. Trivedi, Avadhesh Kumar Gupta, Paritosh Tripathi. "Chapter 20 Current Trends in Cryptography, Steganography, and Metamorphic Cryptography: A Survey", Springer Science and Business Media LLC, 2021 Crossref	22 words — < 1%
11	www.jasonguynn.net Internet	21 words — < 1%
12	www.ijert.org Internet	21 words — < 1%
13	Abdelkader Belhadri, Mohammed Benyettou. "New biometric cryptosystem to protect sensitive data in Internet of objects", Multiagent and Grid Systems, 2018 Crossref	19 words — < 1%
14	M.F. Tolba, M.A. Ghonemy, I.A.-H. Taha, A.S. Khalifa. "High capacity image steganography using wavelet-based fusion", Proceedings. ISCC 2004. Ninth International Symposium on Computers And Communications (IEEE Cat. No.04TH8769), 2004 Crossref	18 words — < 1%
15	Jayanta Kumar Pal, J. K. Mandal, Somsubhra Gupta. "Composite Transposition Substitution Chaining Based Cipher Technique", 2008 16th International Conference on Advanced Computing and Communications, 2008 Crossref	18 words — < 1%
16	www.i-scholar.in Internet	14 words — < 1%
	viola.usc.edu	

17	Internet	14 words — < 1%
18	www.ukessays.com Internet	14 words — < 1%
19	csrc.nist.gov Internet	13 words — < 1%
20	www.oupcanada.com Internet	13 words — < 1%
21	Aruna Malik, Geeta Sikka, Harsh Kumar Verma. "A Modified Pixel-Value Differencing Image Steganographic Scheme with Least Significant Bit Substitution Method", International Journal of Image, Graphics and Signal Processing, 2015 Crossref	11 words — < 1%
22	mafiadoc.com Internet	11 words — < 1%
23	Saumya Batham, Virendra Kumar Yadav, Amit Kumar Mallik. "ICSECV: An efficient approach of video encryption", 2014 Seventh International Conference on Contemporary Computing (IC3), 2014 Crossref	11 words — < 1%
24	www.oralpath.com Internet	10 words — < 1%
25	Ramineni Siva Ram Prasad, Kalavathi Alla. "A new approach to Telugu text steganography", 2011 IEEE Symposium on Wireless Technology and Applications (ISWTA), 2011 Crossref	10 words — < 1%
26	www.tandfonline.com Internet	10 words — < 1%
27	Pramod Pavithran, Sheena Mathew, Suyel Namasudra, Pascal Lorenz. "A Novel Cryptosystem	9 words — < 1%

based on DNA Cryptography and Randomly Generated Mealy Machine", Computers & Security, 2020
Crossref

28 Namrata Singh, Munesh Chandra Trivedi, Virendra Kumar Yadav, Vikash Kumar Singh. "Metamorphic cryptography considering concept of XOR and chaotic sequence: Using video as medium", 2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE), 2017
Crossref
9 words — < 1%

29 "Advances in Neural Networks – ISNN 2007", Springer Nature, 2007
Crossref
9 words — < 1%

30 "Information Systems Design and Intelligent Applications", Springer Science and Business Media LLC, 2015
Crossref
9 words — < 1%

31 www.journal.bonfring.org
Internet
9 words — < 1%

32 Puteri Awaliatush Shofro, Kiki Widia, Dwi Dian Ayu Puji Astuti, Eko Hari Rachmawanto et al. "Improved Message Payload and Security of Image Steganography using 3-3-2 LSB and Dual Encryption", 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018
Crossref
9 words — < 1%

33 link.springer.com
Internet
9 words — < 1%

34 "Computational Intelligence in Data Mining", Springer Science and Business Media LLC, 2019
Crossref
9 words — < 1%

35 Shivani, Virendra Kumar Yadav, Saumya Batham. "Zero Distortion Technique", Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '14, 2014
Crossref
9 words — < 1%

36	dokumen.pub Internet	9 words — < 1%
37	V Geetha, N Laavanya, S Priyadharshiny, C Sofeiyakalaimathy. "Survey on security mechanisms for public cloud data", 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 2016 Crossref	9 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		