Comparatives Analysis of Secure Information Transmission Based on Cryptography Fused with Steganography

Mr. Akash V. Malasane, Prof. S. P. Bhonge

***Abstract*— Metamorphic cryptography is the contradiction between of cryptography and steganography. This combination will be used for the higher level of security has gained a lot of importance. Cryptography refers to the study of art and science for achieving security by encode the messages to make them sure that the data is not readable. The readable message is converted into an unreadable message by using cryptographic system, this process called as well-structured and methodical, exact opposite operation is performed by using cryptanalysis that means unreadable message is converted into a readable message, this process called as miscalculation and trial based. Steganography is the technique that give the skill to hide the massages that is to be kept secret inside other messages. Before The art and science of writing hidden messages in such a way that no one can access this information expect sender and receiver. This paper provides a comparatives study of secure information transmission based on metamorphic cryptography and higher level of security for hide the information video by using development of system for video based metamorphic encryption.**

***Index Terms*— Cryptography, Steganography, AES, LSB, Key.**

I. INTRODUCTION

Everybody know that security of information has become a major anxiety in this day. The security is becoming more important as the volume of data being exchanged from sender to receiver and receiver to sender with proper way. The infringements in universal network environment and in applications the security and privacy of has become progressively more important in today's highly computerized and interconnected world. Security has become the important features in communication and other text information these is because of the presence of hackers who wait for a chances to gain an access to private data. We can service two varied procedures for the information security which are Cryptography and Steganography. This will combine to each other and made up full proof security for high level of security no one can easily access by using development of system for video based metamorphic encryption and application of Steganography technique i.e. LSB (Least Significant Bit) as well as application of Symmetric Key Encryption i.e. AES (Advanced Encryption Standard), and for this algorithm type used by block cipher.

The grouping of cryptanalysis and cryptography called as cryptology. Before cryptography used to be performed by using guide techniques. In today's lots of improvement occurs in real implementation. Computers now perform the cryptographic algorithms and cryptographic application this manufacture the process a lot faster and secure this is one of the most important factor. Human can speak in plain text and not explicit message called as cipher text. In past days cryptography used for the manual techniques to be performed. The basic outline of cryptography for the performance became a same has continued less or more, defiantly with a more developments in the actual implementation. The most important point in that the computer performed this cryptographic functions, from this point of view the process become a more secure and more faster. The basic concept of cryptography is the how we can make information unreadable and protected, this will be done by many ways [10]. Some cryptography algorithms are very easy to understand and therefore this algorithm are easily crack. Some cryptography algorithm are highly complex and therefore difficult to crack.

Steganography pursues to encrypt information, Steganography is a technique that implanting secreted messages that is to be kept secret in such a way that no one can access the data, except the sender and intended receiver can detect the existence of the messages. The main objective of steganography is to hide the secret information in such a way that viewers are not able to detect it. Another one objective of steganography is to be communicate securely in a fully too small to see manner. The numerous forms of data in steganography can be audio, video, text and images. In past decade the sender used the method such as pencil marks on handwritten characters, unseen ink, tiny difference between handwritten characters, little pin punctures on specific characters, etc. Steganography is came from Greek words steganos (covered) and graptos (writing) Steganography is used in various forms for the past 2500[10].In steganography having many techniques are available i.e. printed techniques, physical techniques, network technique and digital technique. In digital techniques again two types such as Injection and Least

Manuscript received July, 2015.

*Mr. **Akash V. Malasane**, EXTC, P. R. Pote (Patil) College of Education & Welfare Trusts Group of Institution. Amravati, Amravati, India, Mobile No: 9096554378.*

***Prof. S. P. Bhonge**, EXTC, P. R. Pote (Patil) College of Education & Welfare Trusts Group of Institution. Amravati, Amravati, India, Mobile No: 9096015952.*

ISSN: 2278 – 1323

Significant Bit (LSB). Again in Steganography various Practical uses i.e. watermarking, branding, alleged use by terrorist and alleged use by intelligence services.

In this proposed method combines two technique steganography and cryptography to provide a very high level security of data such as hide the video information in a video clip by using application of Steganography that is LSB technique and type of algorithm that is block cipher, and also video based metamorphic encryption, decryption technique. That means it's provide higher security level as compare to hide the information in image form, audio form and in a text form by using steganography and cryptography. In that proposed method hacker does not hack data because hide the information video in a video form this is unbreakable.

II. RELATED WORK

Now a day's many algorithms are attainable for security purpose using various encryption technique for example simple preservative cipher techniques in to the complicated asymmetric and symmetric key ciphers techniques by using this we increase the security of information. But hear problem is which technique is fighting fit suitable to protect our data for higher level. If we used various cryptography techniques then we used also cryptanalysis technique and this fusion is called as cryptology. Again we can used various steganography techniques for example LSB technique. This two technique method provide separate as well as mutual security for hiding a data. Cryptography hide the information and it can be transformed into an unintelligible form. It is used in advanced technology application such as ATM card, passwords and etc. This all thing depend on cryptography. Steganography is the method that can used for the hide the messages in such way that avoid the detection of hidden messages [10].

The Authors Dhawal Seth and L Ramanathan. [1] Offer the confederacy of Cryptography and Steganography to improve the security of the data. The text messages that is plain text is first encrypted by using Data Encryption standard with a key produces Codified Text that is cipher text. Added Cipher text is hide by using cover image fused with embedding algorithm that is LSB using a steganography key, crops Steganography Image. This Steganography Image is lastly sent to the receiver. Then if we want original text or plain text decoding and decryption operation perform by using proper key we get original plain text. This paper Author used Data Encryption Standard Symmetric Encryption Algorithm and then LSB techniques.

In this paper [2] Authors defined and studied the numerous research works that has to be done in the path of text encryption and text decryption in the block cipher. Hear proposed system is combined the steganography and cryptography and generate a new technique that is metamorphic cryptography. Furthermore. Cryptography and Steganography reach the same objective in different means. In that paper combines the two techniques (cryptography and steganography). In that paper paradox for encryption and paradox for decryption flow chart show from message to final image and final image to original message respectively. Shortly its procedure is firstly message is to be encrypted in cover image by using encryption paradox method, it's secure in cipher image again in intermediate text and finally we get the final image. Then we want the original message the procedure is reverse that is decrypted intermediate text and then cipher image using the decryption paradox method lastly we get the decrypted original message. This method is strong as compare to other because its provide two times greater security, but in that message hide in image by using steganography so more chances in this method the hacker hack the information.

Khalil Challita et al. [3] present new visions i.e. how to increase surviving methods of hide a secret information, probably by using mixing of steganography and cryptography. This paper authors put forward that both the sender and the receiver approve on a cover image sending a secret message. The procedure does not adjust the cover image, somewhat it finds the bits of the secret message that matching the one of the cover image and stores their different locations that is in the cover image in a vector. This vector is then sent that means probably encrypted using classical cryptography to the recipient. This will be shows that new direction of combination of cryptography and steganography. The proposed procedure are as follows shortly the plain text and cover image is combine and forward to in embedding algorithm by applying steganography key and this will produced steganography image then this image encrypted and gives the cipher steganography image by applying key then if we want the hidden messages then procedure is reverse that is decrypted image by using key we get the steganography image this image again decoded by using steganography key and finally we get the original messages.

In [4], the authors Rosziati Ibrahim, Teoh Suk Kuan proposed in that paper, the user enter their user id and their password for the log-in in the system. After that positively log-in user, user can be insert a secret message into an image by using key and lastly produce steganography image. This same key is use for the receiver side for saving a data. At this time the secret messages is transfer into a text folder. Then this text file is compacted into zip text file, and this zip text file is use for make over into a binary codes. Zip text file is safe and is not easy to detect. The zip file again having one important advantage that is its store the some space hence it is called as the Zip file.

S.S. Divya et al. [5] proposed two state-of-the-art approaches of LSBs of audio samples for data hiding. These methods first check the MSBs of the samples, and then next number of LSBs for data hiding is decided. In that manner, more than a few and variable LSBs are used for embedding secret data. These proposed methods strangely increase the capability for data hiding as compared to standard LSB without causing any noticeable alteration to the data. Authors used both LSB and MSB Algorithm (Steganography) and RSA Algorithm (Public Key Cryptography Technique).Using MSB Algorithm the value of the MSB of the digitized samples of cover audio for data hiding. As paralleled to standard LSB coding method, these methods embedded data in numerous and variable LSBs depending on the MSBs of the cover audio samples. Here authors checks only the MSB of the cover sample. There is a remarkable increase in

ISSN: 2278 – 1323

Capacity of cover audio for hiding additional data and without disturbing the perceptual transparency of the text, provide the keys concept for secure data. The main improvement of this proposed method is that, they are simple in logic and the hidden information is recuperated without any error, thus it succeeds in attaining the basic requirement of data hiding.

In this paper [6] the authors Basant Sah and Vijay Kumar Jha proposed method gives the hide the information inside the image by using the replacement of LSB and MSB technique in that paper, proposed work are as follows first of all find the key that is public key and private key according to RSA algorithm approach and encrypted the secret messages this algorithm is the most popular and proven asymmetric key cryptographic algorithm, RSA methodology and encode secret information. The secret information is encrypted and then encrypted ASCII value is transformed in binary form encrypt the information and then subsequently replace the MSB and LSB bit with information. The pixels image is also converted at the same time into the binary form. The image is used as a cover to insert the encrypted information. This process is finished by least significant bit (LSB) encoder which substitutes the least significant bit of pixel values with the encrypted information bits. In that one disadvantage occurred that is in that paper the time complication of the complete process increase.

In this paper [7] authors Dr. R. Sridevi, et.al proposes a method, which combines the techniques of Steganography and cryptography, to hide the secret data in an image. In the first phase, the sender will embed the secret data in an image by using the Least Significant Bit (LSB) technique. The embedded image will be encrypted by using an encryption algorithm. At final, the encrypted image will be decrypted and the hidden data will be repossessed by supplying the valid secret key by the receiver. The process includes the phases of Data embedding, Image Encryption and recovery of both original image and secret data from the encrypted image. In this paper, Authors proposed the combination of Image Steganography and cryptography has been achieved by using the LSB technique and AES algorithm. LSB technique is used to hide the secret data into an image and AES (Advanced Encryption standard) is used to encrypt the steganography image. From the encrypted image, recovery of the original image and withdrawal of the hidden data operations are performed. Finally Authors conclude in that, the proposed technique is effective for secret communication and provides the better security, but combination of image encryption and data hiding capable with lossy compression.

In this paper [8] implanted vast quantity of secret information using LSB technique (Steganography).To reach first of all this secret information is compressed using wavelet transforms. Then density is done the bits are encoding using an alterable or reversible quantum gate. Least Significant Bit is one of the finest techniques as equated to transformation techniques, because this LSB technique reduces lots of noise distortion and it is use in a digital technique. In steganography algorithm having some limitation are possible for example limited number of ways for hiding data that is the size of the medium limits the quantity that can be successfully in the medium of data from that steganography cannot provide the required security because some limitation of steganography.

In this paper [9] authors proposed scheme is, include assortment of cryptography and steganography to data confidentiality over secrecy there by increase the security level. It is used for the securely interchange private information between administrations. In this author suggests a two steps of security first one is encryption process and second one is steganography increase the security level for data hiding. In first stage message is transmitted and is first of all transformed in to a cipher image by using the first encryption process. Then in second stage this cipher image is to be transformed in to an intermediate text by using the second encryption process. The intermediate cipher text or information created hidden text inside a cover image by using steganography to hidden the presence of the secret and this resultant steganography image is transferred to the receiver done the network. Thus in that paper dual encryption and steganography scheme are proposed the encryption process is fully at the mercy of on a key, encryption process used the RSA algorithm and steganography technique is used for the embedding of the image, steganography used LSB technique.

III. COMPARISIONS WITH OTHER TECHNIQUES

Table 1: Different Techniques use by Authors

Sr. No.	Authors Name	Cryptography Techniques	Steganography Techniques
1	Dhawal Seth,et.al	Symmetric key Encryption	Least Significant Bit
2	Thomas Leontin Philjon. J, et.al	Angular Encryption & Dynamic Encryption	Paradox Encryption
3	Khalil Challita, et.al	Encryption	Least Significant Bit
4	Rosziati Ibrahim, et.al	-	Steganography Imaging System
5	S.S. Divya, et.al	Asymmetric key Encryption	Multiple Least Significant Bit
6	Basant Sah, et.al	Asymmetric key Encryption	Replacement of LSB & MSB
7	Dr. R. Sridevi, et.al	Symmetric key Encryption	Least Significant Bit
8	R Praveen Kumar, et.al	-	LSB Insertion Method
9	A Aswathy Nair, et.al	Asymmetric key Encryption	LSB Steganography Technique
10	Mr. Akash V. Malasane, et.al	Symmetric key Encryption	Steganography Technique (LSB)

Table 2: Different hidden format and algorithms use by Authors

Sr. No.	Authors Name	Where The Information Hide In The Form of Image, Audio, Text, Video.	Algorithm
1	Dhawal Seth,et.al	Image	DES
2	Thomas Leontin Philjon. J, et.al	Image and Intermediate Text	Metamorphic Cryptography
3	Khalil Challita, et.al	Stego Object	-
4	Rosziati Ibrahim, et.al	Image	-
5	S.S. Divya, et.al	Audio	RSA
6	Basant Sah, et.al	Image	RSA
7	Dr. R. Sridevi, et.al	Image	AES
8	R Praveen Kumar, et.al	Image	-
9	A Aswathy Nair, et.al	Image and Intermediate Text	RSA
10	Mr. Akash V. Malasane, et.al	Video	AES

IV. PROPOSED SYSTEM

Our work mainly focuses on providing double layer security for the Video using Metamorphic Cryptography. Each frame of the video is first Encrypted using Symmetric Key; each frame of the encrypted video is further concealed with cover image resulting into Steganography image. In such a way all frames of encrypted video is steganography. Finally the set of all Steganography images (Steganography Encrypted Video) is sent to the receiver. Our proposed Metamorphic Cryptography model is as follows. Again this metamorphic cryptography also called as paradox between cryptography and steganography. Bellow shows the Metamorphic Encryption and Decryption Techniques flow chart for Video.

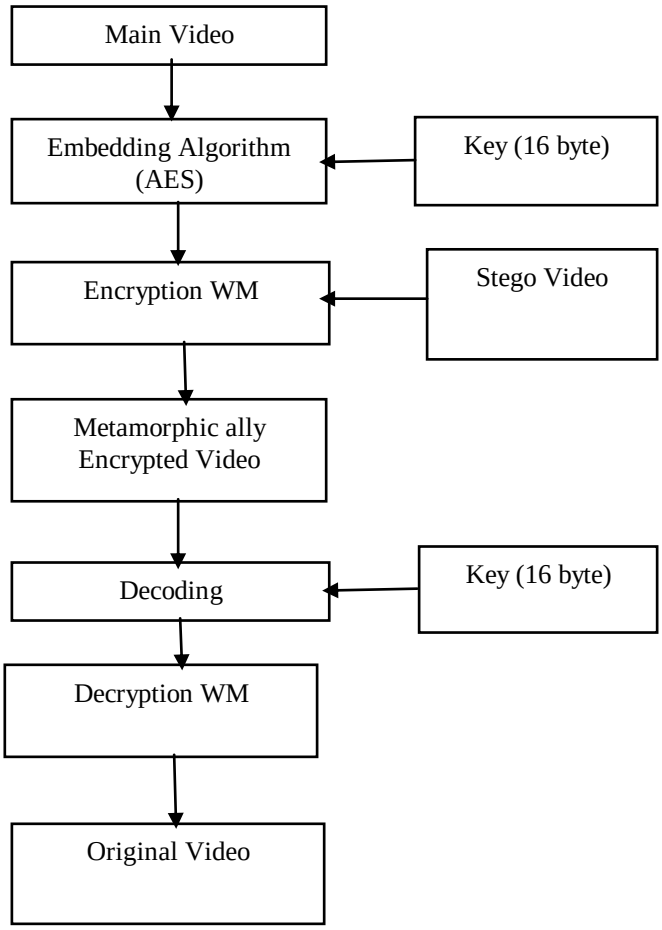

Fig.1: Flow chart of Metamorphic Cryptography for Videos

A. Working Principle of AES Algorithm

- Key Expansion: Using key expansion Round keys are derived from the encryption key using Rijndael's key Schedule.
- Initial Round
  - Add Round Key: Round key and each byte of the state is combined using bitwise XOR.
- Rounds
  - Sub Bytes: It is a non-linear substitution step where each byte is replaced with another byte according to a lookup reference table.
  - Shift Rows: It is a transposition or permutation step. In this step each row of the state is Shifted Cyclically a certain number of steps.
  - Mix Columns: It is a mixing Operation, Which operates on the Column of the State, and combining the four bytes in each column.
- Final Round (no Mix Columns)
  - Sub Bytes
  - Shift Rows
  - Add Round Key

The based file video and cover file video details are given in and also results are tabulated in Table 3.

Table 3: Based and Hidden Video File Details and Result Obtained from AES Algorithm and LSB Technique.

Sr. No.	Name of Video	W*H	Frame Rates	Data Rate
1	almov5.avi (Base Video)	160*120	15 Frames/Second	60kbps
2	almov6.avi (Cover Video)	160*120	15 Frames/Second	60kbps

Thus from this above information we can calculate the PSNR and number of Frames required for hiding the data thus this are as follows.
Total Frames. = **108.**
PSNR (Peak Signal to Noise Ratio) = **48.22dB.**
To compute the PSNR, first calculates the Minimum Mean Squared Error using the equation number 1.

$$MMSE = \sum_{M,N} \frac{[I1(M,N) - I2(M,N)]^2}{M * N}$$

……..Eq. No. 1.

M and *N* are the number of rows and columns in the input images, respectively. Then the computes the PSNR using the equation number 2:

$$PSNR = 10\log_{10}(R^2/MMSE)$$ ……..Eq. No. 2.

R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.
After encryption and decryption process some changes can be occurred in videos as compare to main video this is shown as bellows.

Table 4: Based and Hidden Video File Details and Result Obtained from AES Algorithm and LSB Technique after Encryption and Decryption process

Sr. No.	Name of Video	W*H	Frame Rates	Data Rate
1	almov5.avi (Base Video)	128*256	30 Frames/Second	1329kbps
2	almov6.avi (Cover Video)	64*64	30 Frames/Second	511kbps

V. CONCLUSIONS

We can conclude that in this paper system is more effective for secret communication over the network channel. In this paper we presented a way of hiding the secret data inside the cover medium such as video. The proposed system for data hiding uses AES for encryption and decryption which generating public key, which results in more secure technique for data hiding. We are using random selection of frames and hide decoy with message also. The security of data is very important, in this paper we surveyed different data hiding techniques. We conclude that all techniques are good for data hiding and have their own advantages and disadvantages and give a security. Combining Cryptography and Steganography is stimulating field and increasing quickly for data hiding in the region of information security. In this project we are concentration on hide information video in another general video by using metamorphic encryption technique so that it will provide high degree Security for the important messages that can be transmitted over the network securely. This paper adventures the techniques of video based metamorphic cryptography the scheme discovered good security for important messages due to its advance technique and its application use over hear. A new algorithm has been suggested that would fulfill all the principles of security and also satisfy the requirements of cryptography and steganography.

ACKNOWLEDGEMENT

We thankful to incalculably our management for outspreading their support in providing us substructure and allowing us to use them in the successful completion of our research paper.

REFERENCESS

[1] Dhawal Seth, L. Ramanathan,"SecurityEnhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010.
[2] Thomas Leontin Philjon and Venkateshvara Rao," Metamorphic Cryptography – A Paradox between Cryptography and Steganography Using Dynamic Encryption", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.
[3] Khalil Challita and Hikmat Farhat"Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208, the Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).
[4] Rosziati Ibrahim, Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application, 2011, pp. 102-108.
[5] S.S. Divya, M. Ram Mohan Reddy, "Hiding Text in Audio Using Multiple LSB Steganography and Provide Security Using Cryptography" International journal of Scientific & Technology Research Volume 1, Issue 6 July 2012, ISSN 2277-8616 68 IJSTR©2012 www.ijstr.org.
[6] Basant Sah and Vijay Kumar,"A New Approach to Data hiding Using Replacement of LSB and MSB" ISSN: 2277 128X Volume 3, Issue 11, November 2013.
[7] Dr. R. Sridevi, Vijya Lakshmi Paruchuri, K. S. Sadasiva Rao. "Image Steganography combined with Cryptography", International journal of computer and Technology Volume 9, No 1.
[8] R.P. Kumar, V. Hemanth, M "Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013, Page(s): 1197 – 1200.
[9] A. Aswathy Nair and Deepu Job,"A Secure Dual Encryption Scheme combined With Steganography" IJETT-Volume 13 Number 5-Jul 2014.
[10] Mr. Akash V. Malasane, Prof. S. P. Bhonge,"Secure Information Transmission based on Cryptography fused with Steganography by using Metamorphic Video Encryption Technique " IJSR-Volume 4 Issue 4, April 2015.

Mr. Akash V. Malasane

Received B.E. degree in Electronics and Tele-Comm. Engineering from DES's COET Dhamangaon Railway in 2013 and currently he is pursuing M.E. (EXTC) degree in P. R. Pote (Patil) College of Engineering. Amravati, Maharashtra, India. His area of interest are Cryptography, Image Processing and ANN.

Prof. Suryakant P. Bhonge

Received M. Tech. Degree and is now assistant professor in P. R. Pote (Patil) College of Engineering. Amravati, Maharashtra, India. His area of interest are Digital Image Processing and ANN.

