International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secure Information Transmission Based on Cryptography Fused with Steganography by using Metamorphic Video Encryption

Akash V. Malasane[1], S. P. Bhonge [2]

[1]Electronics & Telecommunication Engineering, Amravati, P.R.Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati, India)

[2] Professor, Electronics & Telecommunication Engineering, Amravati, P.R.Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati, India

Abstract: ***Metamorphic cryptography is the inconsistency 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 systematic, antithesis operation is performed by using cryptanalysis that means unreadable message is converted into a readable message, this process called as error 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 higher level of security for hide the information messages by using development of system for video based metamorphic encryption***.

Keywords: Cryptography, Steganography, Metamorphic encryption, metamorphic decryption, key.

1. Introduction

In today fast developing area security play the very important role in the daily life and in computer networking. Everybody know that security of information has become a major apprehension in this day and age. 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 encroachments 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. In present Information Security plays a dynamic role. Information are exchanged over a network. 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 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 coded 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 [1]. 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 invisible 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[1].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 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 degree of 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 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 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. As compare to message secure in the form of image, audio and text, in video form gives high degree of security.

2. Literature Survey

Now a day's many algorithms are obtainable 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 well 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 individual as well as combined 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 [6].

The Author Dhawal Seth and L Ramanathan. [2] Offer the grouping 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 i.e. 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 Algorithm.

Mr. Vinod Saroha, et al. [3] This Author Paper innumerable attacks are possible on together asymmetric and symmetric cryptographic techniques such as Brute force attack, Man in the middle attack linear cryptanalysis and etc. Thus From this paper observation we conclude that using only cryptography algorithm/function for data cannot deliver the necessary security. Because hacker access date very easily it cannot be get the guaranty about data. Again Author shows in that paper various cryptanalysis techniques.

In this paper [4] implanted vast quantity of secret information using LSB technique (Steganography).To reach first of all this secret information is compacted using wavelet transforms. Then compression 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 [5] 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) we can say that this technique paradox between them. 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 or output. 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.

In this paper [6] proposed scheme is, include a mixture 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 dependent on a key, encryption process used the RSA algorithm and steganography technique is used for the embedding of the image, steganography used LSB technique.

In this paper [7] the authors suggests image steganography scheme proposed and this scheme based on the List Significant Bit by using replacement method and difference the pixel value. In this proposed method Statistical method hear used in that paper the procedure are as follows encoding the information by varying numerous statistical properties of a cover image and uses a premise testing in the withdrawal process. The overhead process is reached by modify the cover or transforming the cover in that way some statistical characteristics change expressively for example if "1" is transmitted then cover is changed or else it is left as remaining same.

In this paper [8] 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 i.e. 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 surely the time complication of the complete process increase

Khalil Challita et al. [9] present new visions or direction i.e. how to increase surviving methods of hide a secret information or messages, probably by using mixing of steganography and cryptography. This paper author suggested 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 i.e. in the cover image in a vector. This vector is then sent that means probably encrypted using classical cryptography, to the recipient or receiver side. 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 plain text or 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 plain text or original messages.

In [10], the author 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 i.e. hidden 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 transforming into a binary codes. Zip text file is safe and is not easy to detect. In that hear used the zipping. The zip file again having one important advantage that is its store the some space hence it is called as the Zip file. Hear used the image for hiding information so it having less secure as compare to video.

S.S. Divya et al. [12] proposed two innovative methodologies 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, several 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. Author used both LSB and MSB Algorithm (Steganography) and RSA Algorithm (Public Key Cryptography).Using MSB Algorithm the value of the MSB of the digitized samples of cover audio for data hiding. As compared to standard LSB coding method, these methods embedded data in numerous and variable LSBs depending on the MSBs of the cover audio samples. Here author checks only the MSB of the cover sample. There is a remarkable increase in 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 advantage 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.

3. Proposed Methodology

Proposed methodology has been shown in bellow block diagram.

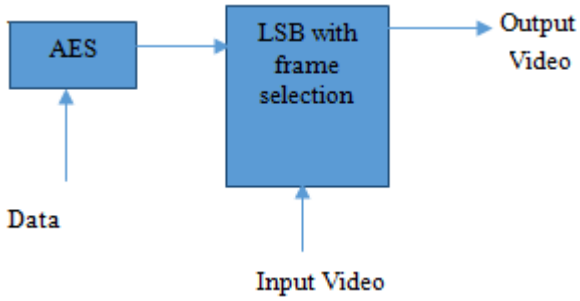

Figure 1: Basic Block Diagram of Proposed Methodology.

Based on discoveries in surviving papers study, new algorithm is being suggested that can make sure all of the security ideologies. We present, in that paper an extra secure information transmission system using double layer security i.e. using cryptography and steganography for improve higher level of security. In above shows a basic model of our proposed methodology. In that first of all we used the block cipher application, like AES (Advanced Encryption Standard) which is apply to data and it will fed to a LSB (Least Significant Bit) with a frame selection using LSB technique for steganography and this block connected to input video applying and we will get a result in a hidden

format i.e. output video this provide higher level of security as compare to text form, image form, audio form.

Now here shows actual implementation, working principle of our suggested paper. 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. Again this metamorphic cryptography say that paradox between cryptography and steganography. In metamorphic encryption technique used two video first one is embedded video called as video1 and second one is the embedding video called as video2 from this proposed method we do the v1 video will be hidden in the v2 video, video is defined as the collection of images or frames. Suppose assume that frames is nothing but, for 1 second 10 frames will done and therefore for 4 second 40 frames run and so on.

Video V1 called as Frame number1 i.e. F1 and Video V2 is called as Frame number 2 i.e. F2 and this paper slogan is, in frame number1 frame number2 is hide. In that paper use the LSB Technique (Least Significant Bit) Steganography. The proposed method procedure are as follows:

1) Data Encryption

First of all we want convert the frame number 1 (F1) into the frame number F1' by using encryption AES (Advanced Encryption Technique) then this F1' follows to F2 and F2 is embedded and get the frame number F2' lastly this F2' is the metamorphic ally encrypted frame. The collection of F2' frames form a video V2' this is the metamorphic ally encrypted videos bellow shows encryption delay per frame procedure in the form of diagram this is as follows:

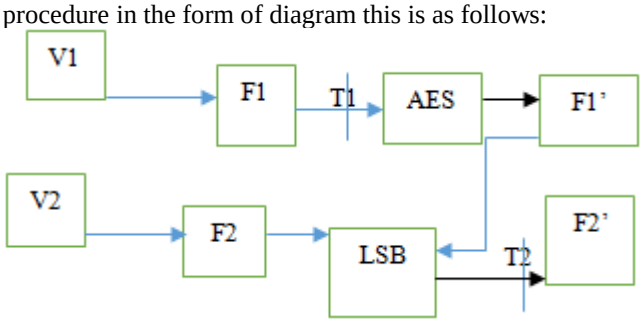

Figure 2: Encryption delay per frame (Delay = T2-T1)

Above is the Data encryption delay per frame in that video 1 and video 2 are converted into frame number that is Frame1 and Frame2 respectively then next F1 is forward to AES (Advanced Encryption Standard), required time is T1 and get the F1' frame then and F2 frame forward to LSB (Least Significant Bit) in LSB F2 and F1' add and getting frame is F2' required time is T2, from this calculate delay i.e. (Delay = T2-T1) then next defined the data decryption, minimum mean square value and lastly peak signal to value this are as follows:

2) Data Decryption

Data Decryption Process is same as the Data Encryption Process only difference is from this find original video and for this procedure is reverse this is shown below figure is as follows:

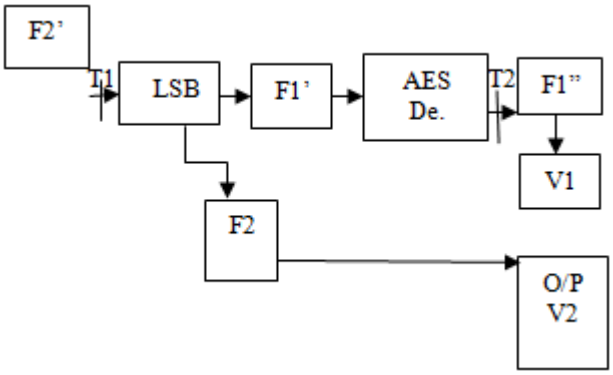

Figure 3: Decryption Delay per Frame. (Delay= T2-T1)

Above figure is the Decryption process for getting the original video and output video from this first of all take the Frame F2' and from this find LSB (Least Significant Bit) required time for this is T1 then from LSB get the two frame i.e. Frame F1' and Frame F2, F2 is nothing but the output video, for the F1' goes to AES (Advance Encryption Standard) decryption Process get the Frame F1" this nothing but the ratio i.e. PSNR verses Frame number. For find F1" required time is T2, again from this find the delay i.e. (Delay=T2-T1).

3) MMSE (Minimum Mean Square Error) and PSNR (Peak Signal to Noise Ratio)

The PSNR block computes the peak signal-to-noise ratio, in Decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error. To compute the PSNR, the block first calculates the mean-squared error using the following equation number 1:

MSE= ∑ [I1 (m,n)-I2(m,n)]^2/M*N
M, N eq.no. (1)

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

PSNR= 10log10(R^2/MSE) 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.

4) Final Window Output

In that figure we observe that first perform the encryption technique, in that the first video take a click is equal to 203 frame numbers, this are depend on the size of the video. Then take an embedding video means that this video hide inside the first video this video we can say that embedding frames, in next steps encrypted this video by using the watermarking process and finally we get the metamorphic encryption frame with time needing for this whole operation.

Then finally do that or perform the decryption operation in that first take an original watermark with a frame number is equal to 203, then this original watermark decrypted by using the PSNR (Peak Signal to Noise Ratio), this value get in decibel form (dB) and for this calculation we required the MMSE (Minimum Mean Square Error) and total image value, above shows a formula of MMSE and PSNR. Finally get the original frame with a time needing for this process and lastly get the graphs and graphs is between the PSNR VS Frame Number.

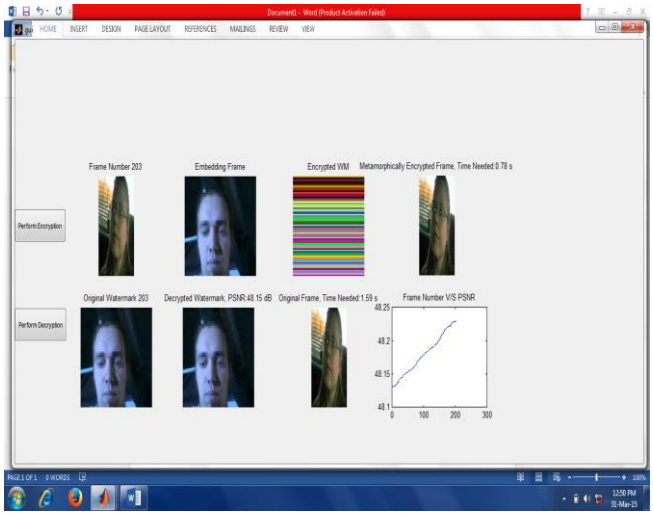

Figure 4: Final Output Window

Thus this is the final output of our proposed method. In that show the actual implementation process with formulas and shows graph between PSNR i.e. Peak Signal to Noise Ratio and the frame number which is required for the video to take a click. Here for this window use technique is graphical user integer (guita) in that use two frame first one is encryption frame and second is decryption frame. In encryption frame having a two parts i.e. first is cipher AES (Advanced Encryption Technique) and next is LSB (Least Significant Bit) Technique. In Decryption Frame again having a two parts, its exact reverse of the encryption frame i.e. Decipher and Inverse LSB Technique.

4. Result

The final result of the our papaer is as shown as bellow for comparative analysis we compare two figures and explain it and also shows the graph, this graph is versus the encryption required time and frame number with table as shown:

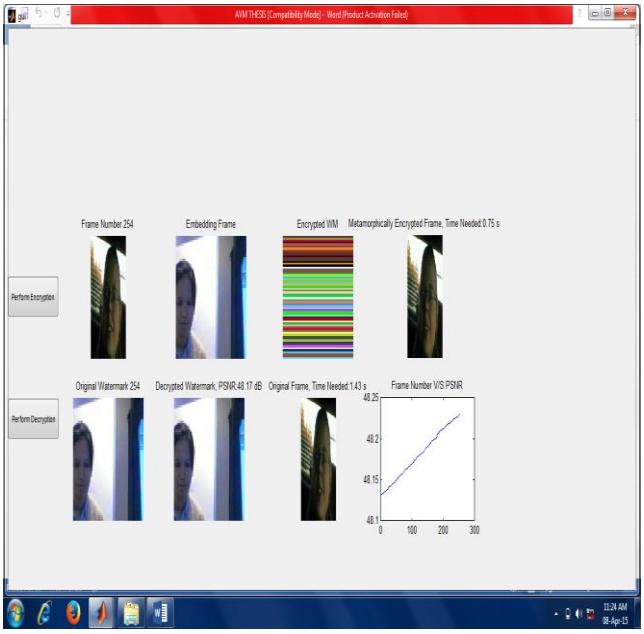

Figure 5: Final Result

This is the final result of our project this windows explain in detail earlier. Thus bellow shows the table and its associated graph, and this contain the frame number, encryption time, decryption time and the Peak Signal to Noise Ratio i.e. PSNR.

Table 1: Values for Frame No. Encryption time, Decryption time and PSNR

Frame Number	*Encryption Time (Te) in Sec.*	*Decryption Time (Td) in Sec.*	*Peak Signal to Noise Ratio (PSNR) in dB*
1	0.63	1.54	48.22
2	0.77	1.38	48.15
3	0.75	1.45	48.17
4	0.67	1.52	48.19
5	0.79	1.40	48.14
6	0.71	1.44	48.19
7	0.64	1.09	48.20
8	0.79	1.32	48.18
9	0.70	1.37	48.14
10	0.76	1.38	48.22
11	0.68	1.43	48.16
12	0.43	1.36	48.23
13	0.74	1.45	48.22
14	0.74	1.40	48.23
15	0.61	1.37	48.15
16	0.74	1.39	48.18
17	0.75	0.97	48.21
18	0.58	1.37	48.18
19	0.75	1.41	48.20
20	0.75	1.43	48.21

Now from this above shown table we can plot the three graph first one is Encryption Time (TE) VS Frame Number (FN), Decryption Time (TD) VS Frame Number (FN) and lastly is PSNR VS Frame Number (FN) but third graph is already plot therefore no need to plot because its already mention in result window output, and we only plot the remaining two plot that is shown as follows:

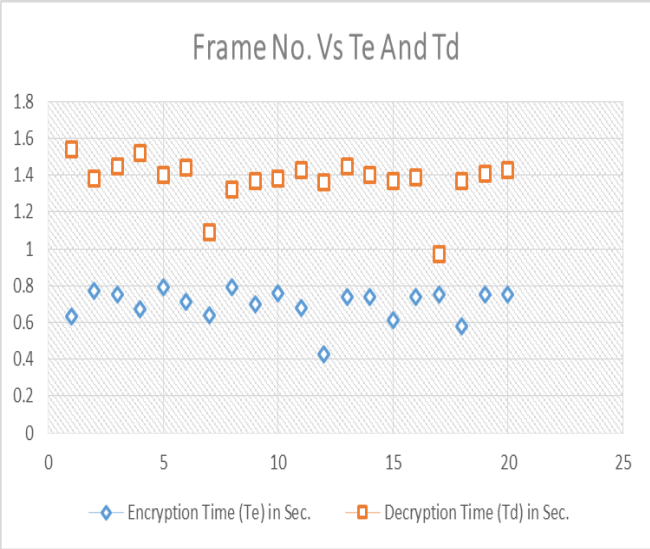

Figure 6: Graph between Frame Number and Encryption, Decryption Time.

5. Conclusion

In today's world where nothing is secure, 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 proposed paper we are concentration on hide information or data in Video form 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 proposed 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.

6. 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.

References

[1] Atul Kahate, Cryptography and Network Security, Second edition.
[2] Dhawal Seth, L. Ramanathan,"SecurityEnhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010.
[3] Mr. Vinod Saroha, Suman Mor, Jyoti Malik,"A Review of Various Techniques of Cryptanalysis", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, ISSN: 2277128X, IJARCSSE October 2012.
[4] 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.
[5] 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.
[6] A Aswathy Nair and Deepu Job,"A Secure Dual Encryption Scheme combined With Steganography" IJETT-Volume 13 Number 5-Jul 2014.
[7] H.C. Wu, N.I Wu, C.S. Tsai and M.S. Hwang, "Image Stenographic scheme based on pixel-value differencing and LSB replacement methods", VISP(152), No. 5, October 2005.
[8] 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.
[9] 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).
[10] Rosziati Ibrahim, Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application, 2011, pp. 102-108.
[11] Sheila Jeruto Magut "An Overview of Digital Steganography"CS5910 Fall 2010 UNIVERSITY OF COLORADO AT COLORADO SPRINGS, COLORADO SPRINGS, COLORADO.
[12] 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.

Author Profile

Mr. Akash V. Malasane received the B.E. degree in Electronic and Telecommunication Engineering from DES's COET Dhamangaon railway Amravati University in 2013. He now Pursuing M.E. Degree from Amravati University.

Prof. Suryakant. P. Bhonge received the M Tech degree in Amravati Government College. He now with Lecturer in P. R. POTE (PATIL) Welfare & Education Trust's college of Engineering & Management, Amravati, India.