A Review on Metamorphic Cryptography for Video Files

[1]Dhananjay M. Dumbere, [2]Nitin J. Janwe

[1, 2] Computer Science and Engineering, Gondwana University, R.C.E.R.T
Chandrapur, Maharashtra, India

Abstract- Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Steganography is the science of embedding information into the cover image viz., text, video, and image without causing statistically significant modification to the cover image. Combining these two techniques either way together result to new technique-Metamorphic Cryptography [14]. The data (text, audio, video, images) is transformed into cipher data using a key, concealed into another cover object (audio, video, images) using Steganography converting it into a Stegno object, and is finally sent to the receiver. Or the data (text, audio, video, images) is concealed into Cover Object resulting into Stegno Object, (Steganography)and further converting Stegno Object into Cipher Stegno Object (audio, video, images) using Cryptography, and is finally sent to the receiver. This proposed both the technique thus achieves double layer security to data.

Keywords - *Metamorphic Cryptography, Cover object, Stegno object, Cipher Stegno Object, Cryptography, Steganography*

1. Introduction

Due to the advancements in ubiquitous network environment and rapid developments in cloud computing has promoted the rapid delivery of digital multimedia data to the users. Multimedia data (images, videos, audios, etc.) are of importance for use more and more widely, in applications such as video-on-demand, video conferencing, broadcasting, etc. Now, it is closely related to many aspects of daily life, including education, commerce, defense, entertainment and politics. Hence the security and privacy of videos has become increasingly more important in today's highly computerized and interconnected world. Digital media content must be protected in applications such as pay-per-view TV or confidential video conferencing, as well as in medical, industrial or military multimedia systems. With the rise of wireless portable devices, many users seek to protect the private multimedia messages that are exchanged over the wireless or wired networks.

The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking cipher text; that is seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. Modern cryptologists are generally trained in theoretical mathematics—they have to be.

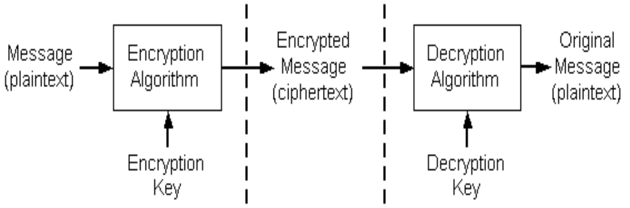

Fig. 1: The schematic of cryptographic operation

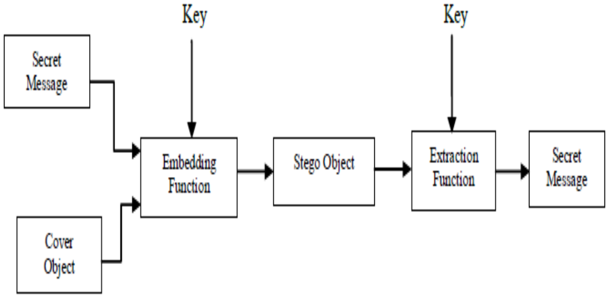

Fig .2: The schematic of steganographic operation

Steganography is the technique of hiding confidential information within any media. Steganlysis is process to detect of presence of steganography. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data with another".

The rest of the paper is organized as follows. Section 2 describes the Literature review by the researchers, Section 3 we will discuss on our proposed work, and finally we draw some conclusion in Section 4.

2. Literature Review

Dhawal Seth et al. [1] first propose the combination of Cryptography and Steganography to enhance the security of the data to be sent. The text data (plain text) is first encrypted produces Cipher Text.Futher Cipher text is then concealed with cover image, produces Stegno Image. This Stegno Image is finally sent to the receiver. Author used DES Symmetric Encryption Algorithm (Cryptography) and then LSB Algorithm (Steganogarphy). The proposed model is as follows:

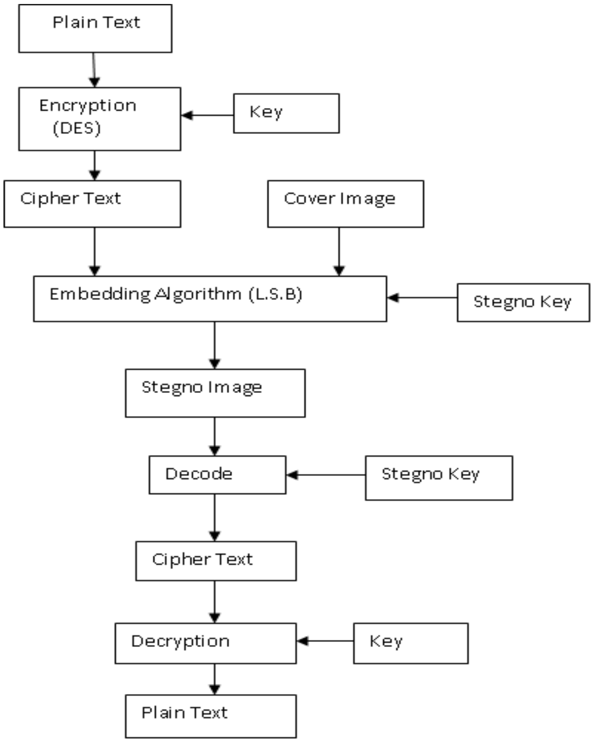

Fig.1. Combining Cryptography and Steganography

Shouchao Song et al. [2] proposed a new secure communication protocol that combines steganography and cryptography techniques .It is based on the LSB matching method and the well-developed Boolean functions in stream ciphers. The cover media employed focuses on grayscale images, and the Boolean function is used for encryption and controlling the pseudo-random increment or decrement of LSB. Unlike the existing methods of doing encrypting and hiding separately, this protocol is one-stop, accomplishing them all at once. Therefore, it needs less computation than the existing methods do while maintaining high secure quality. This is the first secure protocol of this kind. And this method not only is easy to be implemented, but also has almost optimal embedding ratio, what's more, it is highly robust to resist regular steganalysis, such as RS analysis, GPC analysis, $\chi 2$ –analysis. In this paper, authors partially borrow the idea of LSB Matching and the usage of Boolean functions in stream cipher. Before presenting protocol, author recalls the basic concepts, denotation and properties of LSB Matching method and Boolean functions [3-6].

Khalil Challita et al. [7] introduce new insights and directions on how to improve existing methods of hiding secret messages, possibly by combining steganography and cryptography. Author proposed that both the sender and the recipient agree on a cover image to send a secret message. The protocol does not modify the cover image, rather it determines the bits of the secret message that match the ones in the cover image and stores their different locations (i.e. in the cover image) in a vector. This vector is then sent (possibly encrypted using classical cryptography) to the recipient. The proposed model is as follows:

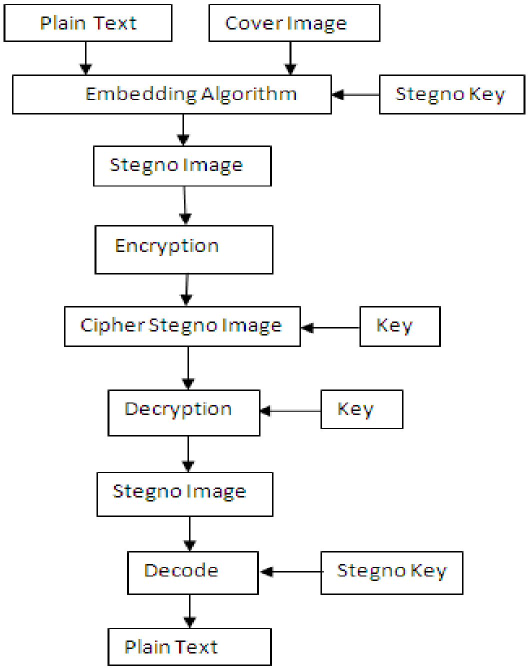

Fig.2. Combining Steganography and Crtyptography

S.S. Divya et al. [8] proposed two novel approaches of LSBs of audio samples for data hiding. These methods check the MSBs of the samples, and then number of LSBs for data hiding is decided. In this way, multiple and variable LSBs are used for embedding secret data. These proposed methods remarkably increase the capacity for data hiding as compared to standard LSB without causing any noticeable distortion to the data [15].Author used both LSB and MSB Algorithm (Steganography) and Public Key Cryptography (RSA Algorithm).Using MSB Algorithm the value of the MSB of the digitized samples of cover audio for data hiding. [16]. As compared to standard LSB coding method, these methods embedded data in multiple 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 affecting the perceptual transparency of the Text. And provide the keys concept for secure data. The main advantage of this proposed method is they are simple in logic and the hidden information is recovered without any error. Thus it succeeds in attaining the basic requirement of data hiding.

Vikas Tyagi et al. [9], this paper discussed a technique based on the LSB (least significant bit) and a encryption algorithm. Author proposed an idea that by matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it. The proposed model is as follows:

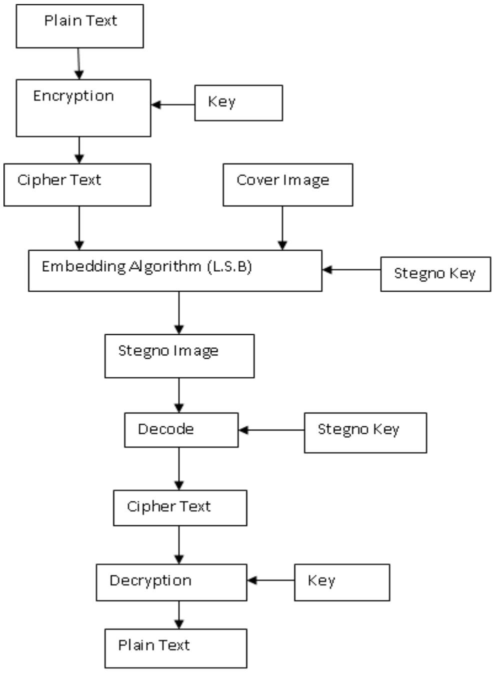

Fig.3. Combining Cryptography and Steganography

Gajendra Singh Chandel et al. [10] proposed a new encryption model by analyzing the principle of the encryption process based on cryptography and steganography. Moreover, the security and performance of the proposed model is also estimated. Author presented results based on combination of cryptography and Steganography approve the effectiveness of the proposed model, and the combination of cryptography and steganography shows advantages of large key space and high-level security. The cipher text generated by this method can be varying in size as the plaintext and will suitable for practical use in the secure transmission of confidential information over the Internet. The strength of the proposed model resides in the new concept of key image. Involving two values (the cover image and the key value) in place of only one (the cover) probably we will be able to change the cover coefficients randomly at the time of implementation of the proposed model. This opportunity does not give a steganalytic tool the chance of searching for a predictable set of modifications. The proposed approach has many applications in hiding and coding messages within standard medias, such as images or videos. The proposed model is as follows

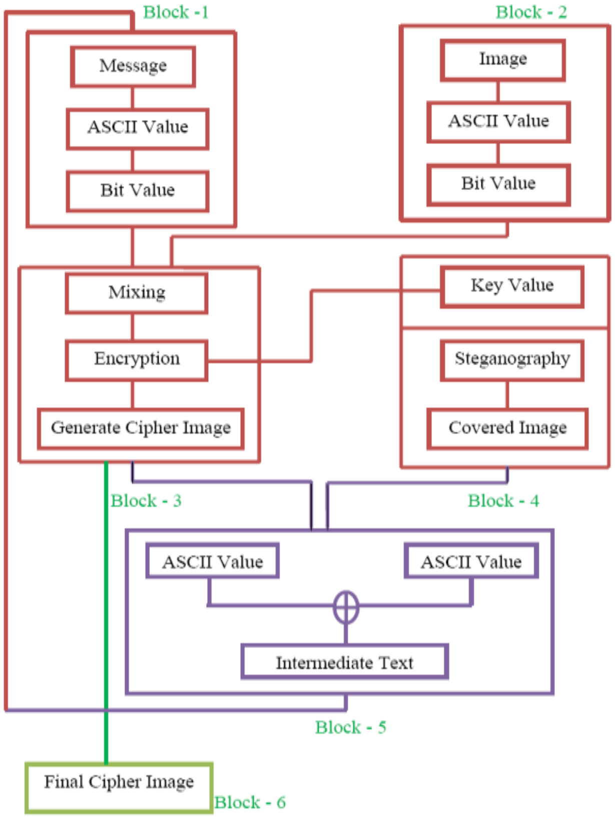

Figure 4: Block Diagram of Proposed Model

Abikoye Oluwakemi C et al. [11] in this paper, a data hiding system that is based on audio steganography and cryptography is proposed to secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file. The proposed system was evaluated for effectiveness and the result shows that, the encryption and decryption methods used for developing the system make the security of the proposed system more efficient in securing data from unauthorized access. An audio medium was used for the steganography and the Least Significant Bit algorithm was employed to encode the message inside the audio file. This proposed system does not tamper with the original size of the file even after encoding and also suitable for any type of audio file format. The encryption and decryption techniques used with this system make its security more robust. The Proposed model is as follows:

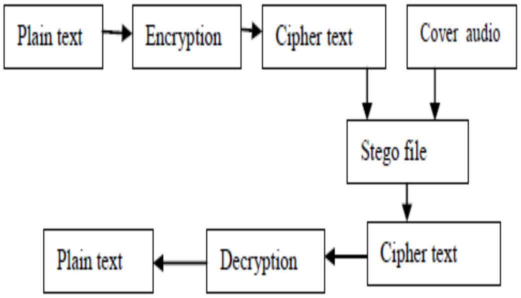

Fig.5. Combining Cryptography and Steganography

Yohan Suryanto et al. [12] proposed Dual Key Triple Encryption Text Based Message Using Cryptography and Steganography is a modular encryption and decryption method for any type of file. It combines layer 1 and layer 2 encryption techniques with standard encryption like AES as layer 3 encryption. Dual symmetric key is required to encrypt or decrypt file, so it can be used by two different persons to encrypt or decrypt certain file. Layer 1 and Layer 2 can use independently to achieve higher security level and fast encrypt or decrypt processing time. We propose character mapping and window addition for level 1 encryption. This technique has better processing time more than 21 times faster than fair character mapping. For layer 2 encryption, we propose scrambling transpose position and dummy file insertion as steganography technique. This method has higher efficiency ratio compare to LSB technique. We can achieve 50% efficiency compare to 12.5% in LSB technique. Combining both methods, we can achieve higher security level by maintaining faster processing time and reduce chipper text size. It can also be used together with AES to increase security level, yet still maintaining fast overall processing time and high efficiency ratio.

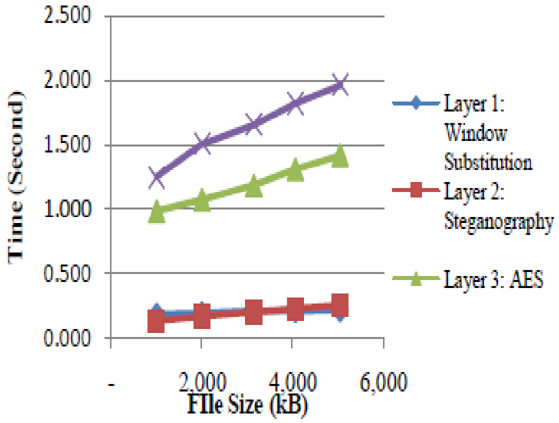

Fig.6. Comparison of processing time for each encryption level.

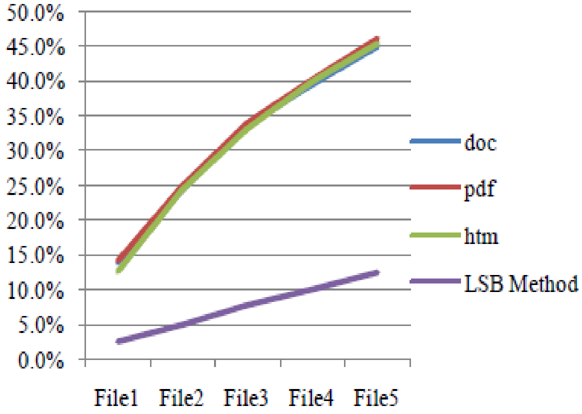

Fig.7. Comparison of layer 2 Steganography and LSB Method

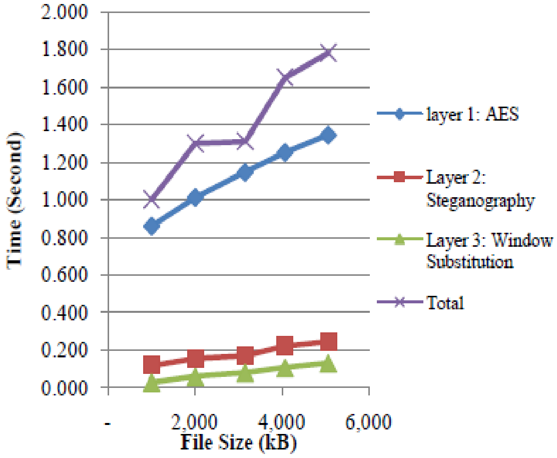

Fig.8. Comparison of processing time for each decryption level.

Using Dual Key Triple Encryption program, proposed layer 1 encryption can achieve much faster time than fair character mapping. This technique has better processing time more than 21 times faster than fair character mapping. In decryption process the same method can achieve about 20 times faster than fair character mapping. Proposed steganography technique in layer 2 encryption has higher efficiency compare to LSB method.. Author has achieve 50% efficiency compare to 12.5% in LSB technique. Combining both proposed methods, higher security level is achieve by maintaining faster processing time and reduce chipper text size. It can also be used together with AES to increase security level, yet still maintaining fast overall processing time and high efficiency ratio. Employ layer 1 and layer 2 encryption to AES encryption process, only take 25 % of total overall process. Mean while in decryption process only take less than 22% of the overall process.

Dr.R.Sridevi et al. [13], 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 retrieved 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 the proposed method, before the hiding process, the sender must select the image of size 512*512 and select the secret message as well as secret key. Secret data hidden into the cover image using the LSB embedding technique. Stego-image which contains the hidden secret data is encrypted using the AES (Advanced Encryption Standard) encryption algorithm. Then the sender may send the encrypted image to the receiver. Receiver applies the decryption algorithm to get the original image and supply the same secret key to retrieve the secret message. In this paper, a specific secret-key image based data hiding model has been proposed which uses an image as the cover object and secret information is embedded into the cover image to form the stego image. Stego image is encrypted in the next step. From the encrypted image recovery of the original image and extraction of the secret data operations are performed. In this paper, author 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 stego image. From the encrypted image, recovery of the original image and extraction of the hidden data operations are performed. The proposed model is as follows:

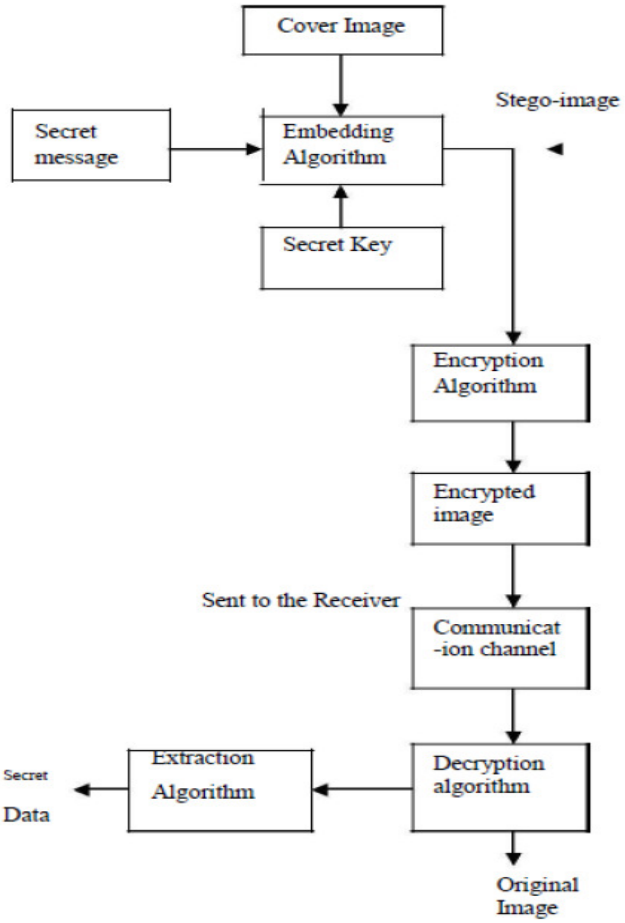

Fig.9. Process of Image Steganography with Cryptography

Thomas Leontin Philjon et al. [16] the method used in this paper is matrix multiplication using a color key along with angular encryption during the encryption process. The ASCII value of each character of the message is taken into account to perform manipulations to produce the cipher image. The cipher image is then concealed using a cover image using steganographic technique and is converted into an intermediate text. This intermediate text is once again encrypted using the encryption technique as proposed above to obtain another image which is the final image. This image is sent to the receiver through the network. The receiver obtains the image, decrypts it to obtain the intermediate text and analyses this text with the cover image to reconstruct the cipher image. This cipher image is once again decrypted to obtain the original message. Proposed idea is as follows:

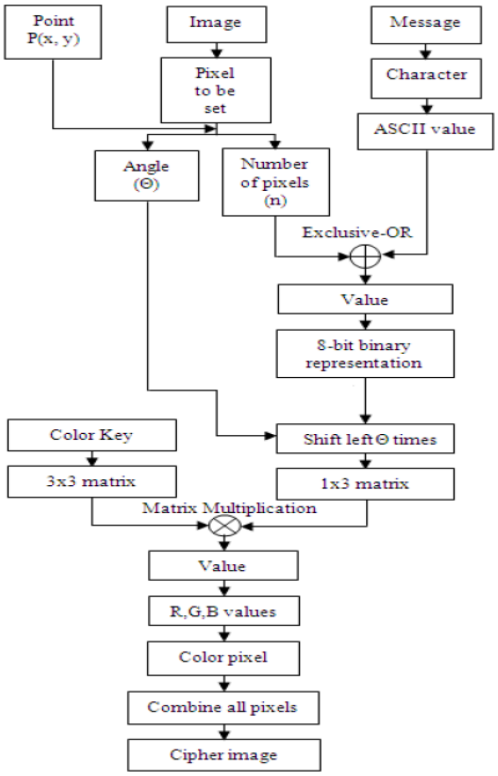

Fig.10.Block Diagram of Encryption

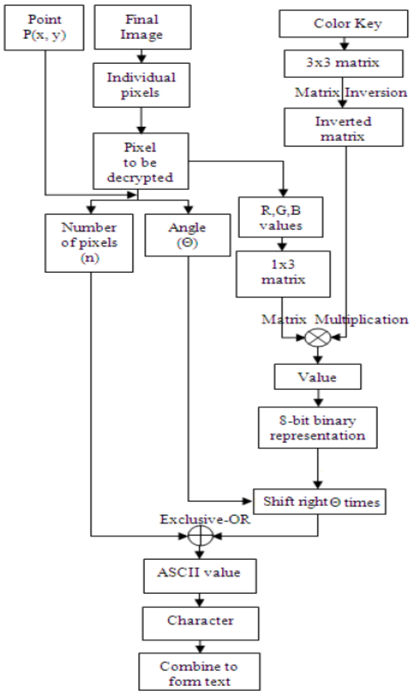

Fig.12.Block Diagram of Decryption

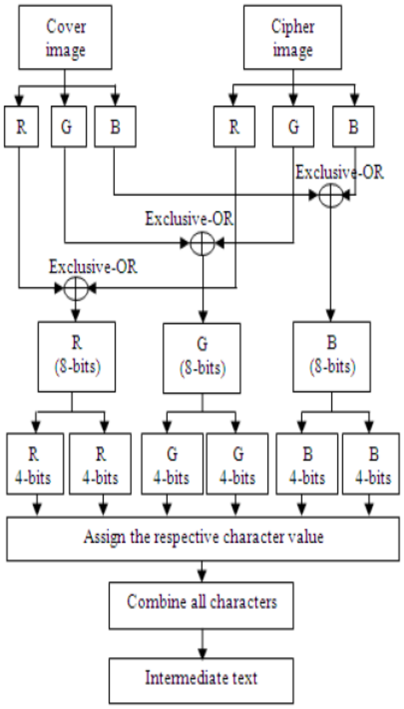

Fig.11.Block Diagram of Steganography

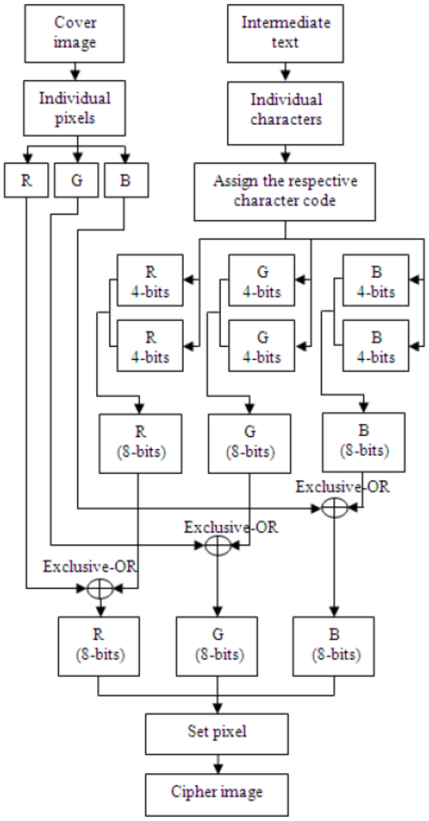

Fig.13.Block Diagram of Retrieval of Cipher Image

3. Proposed Work

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 Stegno image. In such a way all frames of encrypted video is steganograph. Finally the set of all Stegno images (Stegno Encrypted Video) is sent to the receiver. Our proposed Metamorphic Cryptography model is as follows:

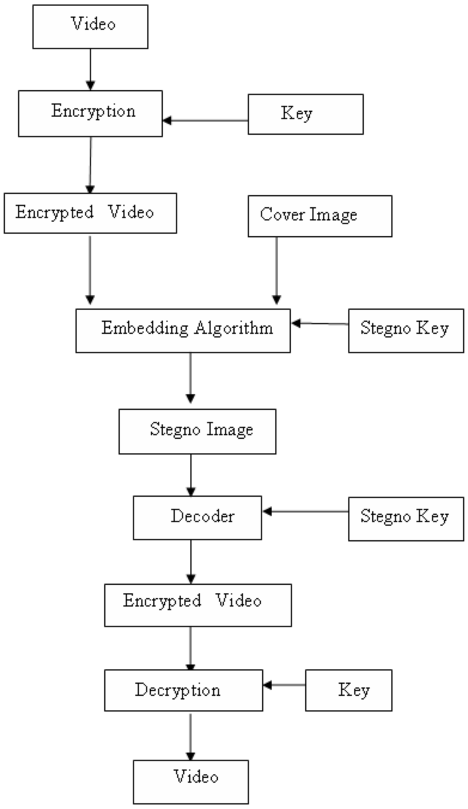

Fig. 14. Block Diagram of Metamorphic Cryptography for Videos

4. Conclusions

Combining Cryptography and Steganography is interesting field and growing rapidly for information hiding in the area of information security.It has a vital role in defence as well as civil applications. Cryptography can be used along with Steganography to make a highly secure data high in the interest of the military. However, Steganography has its place in security. Though it cannot replace cryptography totally, it is intended to supplement it. Video files have not been combined with Cryptography and Steganogarphy yet; hence we are focus on Video files using Metamorphic Cryptography so that to provide full proof Security for the videos that can be transmitted over the network securely.

References

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

[2] Shouchao Song, Jie Zhangb,Xin Liao,Jiao Du Qiaoyan Wen, “A Novel Secure Communication Protocol Combining Steganography and Cryptography”, 2011 Published by Elsevier Ltd. Selection and/or peer-under responsibility of [CEIS 2011] In Advanced in Control Engineering and Information Science.

[3] T. Sharp.” An implementation of key-based digital signal steganography”. Proc. 4th. Information Hiding Workshop, LNCS, vol. 2137, Berlin: Springer-Verlag, 2001, pp. 13–26.

[4] W.C. Thomas, S. Pantelimon. “Cryptographic Boolean functions and applications”, Elsevier: Academic Press, first edition 2009, pp.119-156.

[5] S.S. Song, J. Zhang, J. Du, Q.Y . Wen.”On the construction of Boolean functions with optimal algebraic immunity and good other properties by concatenation”, Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on, Volume1, pp: 417 – 422.

[6] C. Carlet, K. Q. Feng.”New balanced Boolean functions satisfying all the main cryptographic criteria ” [EB/OL]. http://eprint.iacr.org/2008/244.pdf.

[7] 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).

[8] 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 Reseaech Volume 1,Issue 6,July 2012, ISSN 2277-8616 68 IJSTR©2012 www.ijstr.org.

[9] Mr . Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar,” Image Steganogarphy Using Least Significant Bit with Cryptography”,Journal of Global Research in Computer Science, Reaearch paper Available Online at www.jgrcs.info © JGRCS 2010, Volume 3, No. 3, March 2012.

[10] Gajendra Singh Chandel, Ravindra Gupta, Swati Jain,” Proposed Model of Dynamic Encryption using Steganography”, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 9, September 2012) .

[11] Abikoye Oluwakemi C,Adewole Kayode S,Oladipupo Ayotunde J.” Efficient Data Hiding System using

Cryptography and Steganography" International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.11, December 2012 – www.ijais.org.

[12] Yohan Suryanto,Nur Hayati,Hendra,Kusumawardhana, Dr. Riri Fitri Sari," Dual Key triple Encryption Text Based 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,

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

[14] Thomas Leontin Philjon. , Venkateshvara Rao. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption",IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011,

[15] K. Gopalan, "Audio steganography using bit modification", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2009.

[16] C. C. Chang, T. S. Chen and H. S. Hsia, "An Effective Image Stenographic Scheme Based on Wavelet Transform and Pattern- Based Modification", IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

Dhananjay M. Dumbere graduated from Rajiv Gandhi college of Engineering Research and Technology in 2004.
Pursuing M.Tech degree in Computer Science and Engineering from same department, with six years of Academic experience, presently working in Rajiv Gandhi College of engineering Research and Technology as an Assistant Professor in the department of Information Technology. My area of interest includes Cryptography and Network Security, Software Engineering.

Nitin J.Janwe graduated from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nandeed.Completed M.Tech CSE from G.H Raisoni College of engineering, Nagpur. Pursuing PhD form Nagpur University, with nineteen years of Academic experience currently he is Associated Professor at Rajiv Gandhi college of Engineering Research and Technology, guided many UG & PG students. His research areas include Image and Video Processing, Operating System, Computer Vision.