ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

A Novel Information Security Scheme by Creptic Video Stegnography

Siddharth Tiwari[1], Prashant Kumar Koshta[2]

Abstract : **With a successive development of multimedia technology more and more data not only generated but also transmitted too, in several fields some of them are military fields, medical fields etc which should secure their information therefore security and privacy both are important. In this paper a description of a system where video and document files both are important and should be secure. This system give an idea for successfully achieve secure information and efficient communication. We make a combination Stegnography and Cryptography for achieving efficiency (in terms of encryption speed, security and stream size) and flexibility (Platform), It is a challenge or future scope for researches. stenograph video with text(Using Least significant bit algorithm) then applying any multimedia encryption algorithm over stegno-data, so receiving end perfrom reverse operation to decrypt the information.**

Keywords
Steganography, cryptography, Least Significant Bit Algorithm(LSB), Video Encryption Algorithm.

I. INTRODUCTION

Steganography is a data hiding technique that has been widely used in information security where as cryptography is also use in digital communication for same purpose of information security, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication however the communication will be known to everyone. Cryptography protects information by transforming it into an unreadable format. It is useful to achieve confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm.Only those who possess a secret key can decipher (decrypt) the ciphertext into plaintext. Steganography(from Greek, it means ”covered writing”) transmits data by embedding messages into innocuous-looking cover objects, these objects may be video or any multimedia file like image, audio and video both techniques are separately used but some instances will critical when both objects are important and should hidden from external environment for example in video recording (Defense fields) when video and files both are important at that time the purposed approach of cryptic-video Steganography system will be very useful for save the video and data. The basic idea is started from Steganography The majority of today’s steganographic systems uses multimedia objects like image, audio and video etc as cover media because people often transmit digital pictures over email and other internet communication. Depending upon the nature of cover object. Followed by a proper video encryption algorithm so that file automatically save from unwanted access one can use a proper compression scheme for efficient channel utilization. To get the original information at the receiving end a reversal approach is performed where encryption algorithm converted into decryption algorithm and stag-video is decoded and get back separated.

II. DEFINATION AND TERMINOLOGY

Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer **Cryptanalysis** is the reverse engineering of cryptography—attempts to identify weaknesses of various cryptographic algorithms and their implementations to exploit them. Any attempt at cryptanalysis is defined as an attack.

Cryptology encompasses both cryptography and cryptanalysis and looks at mathematical problems that underlie them.

Cryptosystems are computer systems used to encrypt data for secure transmission and storage.

Plaintext is message or data which are in their normal, readable (not encrypted) form.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

Encryption Encoding the contents of the message in such a way that hides its contents from outsiders.

Cipher text results from plaintext by applying the encryption key.

Decryption The process of retrieving the plaintext back from the cipher text.

Key Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.

Steganography is the method of hiding secret messages in an ordinary document.

Steganalysis could be simply defined as the detection of steganography by a third party.

Hash functions generate a digest of the message.

Substitution cipher involves replacing an alphabet with another character of the same alphabet set. Mono-alphabetic system uses a single alphabetic set for substitutions. Poly-alphabetic system uses multiple alphabetic sets for substitutions.

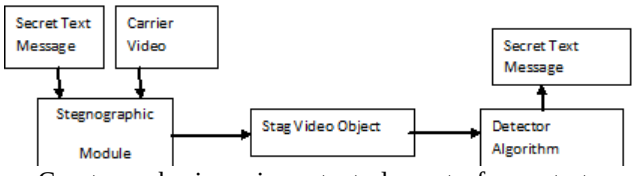
Caesar cipher is a mono-alphabetic system in which each character is replaced by the third character in succession. Julius Caesar used this method of encryption.

III. RELATED WORK

A lot of research is being done in the field of steganography and compression. KB Raja et. al proposed a high capacity wavelet steganography (HCWS) algorithm. The cover image in this model is transformed to wavelet Domain and the payload is encrypted using a random technique to increase its security. Juneja et. Al proposed a robust image steganography technique based on Least Significant Bit insertion and RSA encryption technique. They used the method of ranking a set of images in a library based on their suitability to be used as a cover or carrier. Weifeng Sun Nan Zhang et. al proposed StarNT, a dictionary-based fast and lossless text transform algorithm.

IV. PROPOSED SYSTEM

In this paper the problem of unauthorized data access is minimized by combining cryptography and steganography one implicit method for channel utilization is compression so system compress the cryptic video-steg data now one issue arise here that is sequence of techniques (Steganography, Cryptography and compression) cryptography and compression respectively followed by Steganography is far better combination as compare to vice versa system because in that one position of both stegnography algo and encryption change that case also considerable but two encryption algorithm required in that case one for video stream and another for text so key management is also considerable so this approach is not an intelligent way to combining both techniques. The Two Conventional approaches Stegnography and Cryptography are shown in the figure 1 and figure 2 respectively. The word **steganography** comes from the Greek Steganos, which mean covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. The main goal or steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [4]. During the process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as “covers” or carriers to hide secret messages.

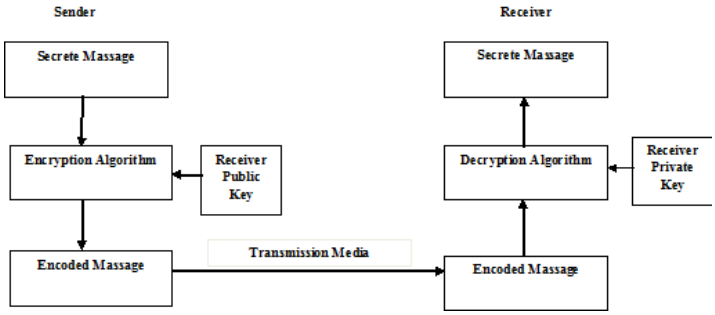


Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'.

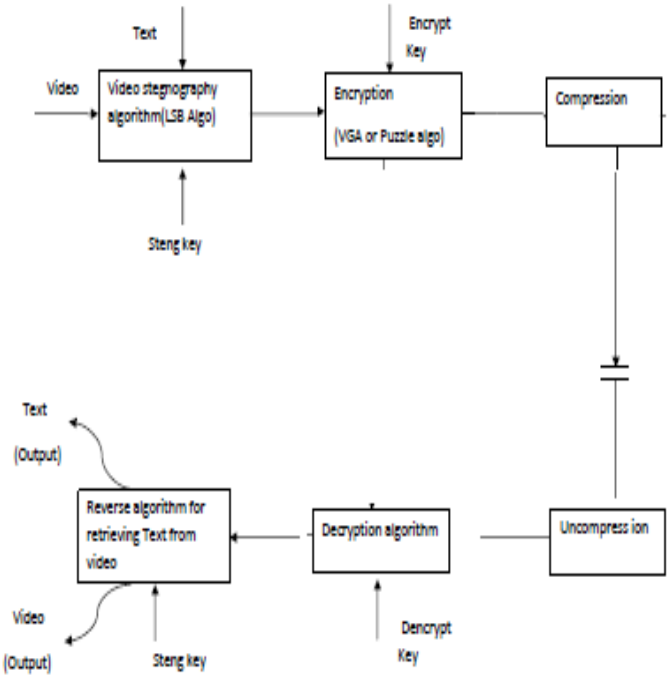
ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

The message may be converted using a 'code' (in which case each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual characters).

Public Key Cryptography (Symmetric) where use same keys in both end (Confidentiality and Authentication leakage) Public Key Cryptography **(**Asymmetric) where different keys use on both end.

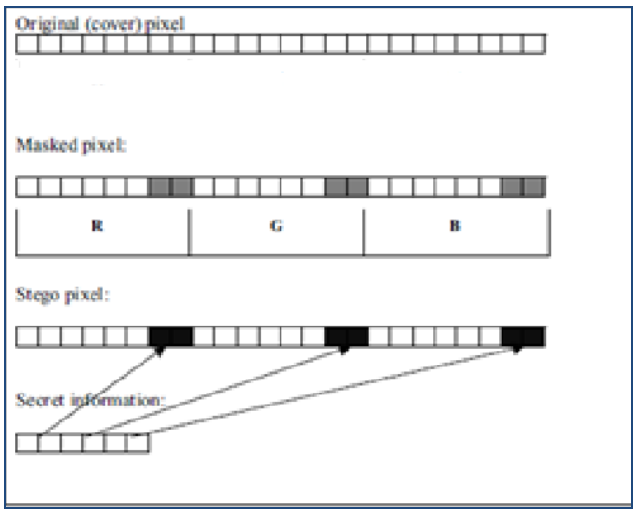


As shown in diagram stegnography followed by cryptography is a new and more secure approach where a lot of data will be save in video and finally both should be secure by Video Encryption Algorithm. The basic purpose of channel utilization is fulfill by lossless compression



Stegnography Algorithm:-

To combine both video and text file a most wide and suitable algorithm least significant algorithm is use. Which are the colored Representations of the pixels are derived from three primary colors: red, green and blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. Using 24-bit images each pixel can represent 16,777,216 color values. We can use the lower two bits of these color channels to hide data, then the maximum color change in a pixel could be of 64-color values, but this causes so little change that is undetectable for the human vision system.



The embedding process of choosing a subset{j1…..,jlm}of cover elements and performing the substitution operation Cji<->Mi on them which change the LSB of Cji by Mi(Can be either 1 or 0) we should be change more than one bit by changing some least significant bits of one cover element. In extraction process the LSB of cover element is extracted and lined up to reconstruct the secrete message. The noticeable point is that size of the embedded data is equal to size of the Video because LSB substitute some Least significant bits from same header (nothing add)

Algorithm: Embedding process LSB Substitution
For i:1……l(c) do
Si<-Ci
End for
For i:1……l(m) do
Compute index ji where to ith message bit
Si< - Ci<->Mi
End for

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

Algorithm: Extraction process LSB Substitution
For i:1……l(m) do
Compute index ji where to ith message bit
Mi<-LSB(Ci)
End for
Now we compress(encryption after compression) the massage after it we can use any video encryption algorithm we use puzzle algorithm for this purpose

Video Encryption Algorithms:- The video encryption algorithms are categorized in following ways and classification is being done by encryption approaches of the frames. The Video Encryption Algorithm (VEA) by Qiaoand Nahrstedt is constructed with the goal to exploit the statistical properties of the MPEG video standard. The algorithm consists of the following four steps:
Step *1:* Let the 2*n* byte sequence, denoted by a1a2…a2n, represent the chunk of an I-frame
Step 2*:* Create two lists, one with odd indexed bytes a1a3…a2n-1, and the other with even indexed bytes *a2a4…a2n*.
Step 3*:* Xor the two lists into an *n*-byte sequence denoted with c1c2…cn
Step 4: Apply the chosen symmetric cryptosystem *E* (for example DES or AES) with the secret key Key E on either odd list or even list, and thus create
the ciphertext sequence c1c2…cn Key E(a1a3…a2n-1) or c1c2…cn Key *E*(a2a4…a2n) respectively. Clearly, the decryption mechanism at the other end of
the communication channel consists of two easy steps: Apply the symmetric cryptosystem *E* with the appropriate key to the second half of the cipher text to
obtain the first half of the original sequence, and xor this result with the first half of the ciphertext to obtain the other half of the original sequence. IT classified into four different video encryption algorithms: Algorithm I, Algorithm II (VEA), Algorithm III (MVEA), and Algorithm IV (RVEA).
The first algorithm, denoted simply by the Algorithm I, uses the permutation of Huffman code words in the I-frames. This method incorporates encryption and compression in one step. The secret part of the algorithm is a permutation, which is used to permute standard JPEG/MPEG Huffman codeword list. In order to save compression ratio, the permutation must be such that it only permutes the Code words with the same number of bits. In addition, the distance between the original and the permuted codeword list must be greater than the encryption quality.

The security of Algorithm I is not particularly good. In, it is shown that the Algorithm I is highly vulnerable to both known-plaintext attack, and cipher text-only attack. If some of the video frames are known in advance (such as standard introductory jingles and similar), one can reconstruct the secret permutation by comparing the original and encrypted frames. The Algorithm II *(*VEA*)* uses the following selective encryption observation: it is sufficient to encrypt only the sign bits of the DCT coefficients in an MPEG video. The Algorithm II simply xors the sign bits ofthe DCT coefficients with a secret m-bit binary key k = k1k2…km. The Algorithm III *(*MVEA*)* is an improvement to the Algorithm II (VEA) described above. It includes the following additions: the sign bits of differential values of motion vectors in P- and B-frames can also be randomly changed. This type of improvement makes the video playback more random and more non viewable.

When the sign bits of differential values of motion vectors are changed, the directions of motion vectors change as well. In addition, the magnitudes of motion vectors change, making the whole video very chaotic. The authors found that the encrypting of sign bits of motion vectors makes the encryption of sign bits of DCT coefficients in B- and P-frames unnecessary.

Finally, the Algorithm IV (RVEA) is significantly more secure approach than the previous three algorithms. This approach is considered to be robust under both ciphertext-only attack and known-plaintext attack. The difference between RVEA and MVEA/VEA algorithms is that RVEA uses conventional symmetric key cryptography to encrypt the sign bits of DCT coefficients and the sign bits of motion vectors. The conventional cryptosystems are well mathematically understood, and thoroughly tested by the experts in the field, which definitely adds on to the security aspect of RVEA. The selective approach significantly speeds up the process of conventional encryption by only.

V. CONCULSION

The work accomplished during this paper can be summarized with the following points :In this paper we have presented a new system for the combination of cryptography and Steganography which could be proven as a better secured method for data communication in near future and we overcome from the conventional use of cryptography and Steganography individually. RVEA only encrypts the fraction (typically about 10%) of the whole MPEG video by using the conventional secure cryptographic schemes such as DES, IDEA, AES, etc.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

Therefore, the Algorithm IV (RVEA) is a much better method than the previous three algorithms in terms of security.

REFERENCES:-

[1] Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo, "Recent Advances in Multimedia Information System Security," International Journal of Computing and Informatics, Vol. 33, No.1, 2009, pp. 3-24.
[2]Sashikala Channalli and Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.
[3] Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm. Available from http://eprint.iacr.org/2004/011.pdf .(Accessed on March 2, 2009).
[4] Shiguo lian, Multimedia Content Encryption: Algorithms and Application, CRC Press, 2008.
[5] Hao Wang and Chong-wei Xu, "A New Lightweight and Scalable Encryption Algorithm for Streaming Video over Wireless Networks", International Conference on Wireless Network, 2007, pp. 180-185.
[6] Shunjun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo, "On the Design of Perceptual MPEG Video Encryption Algorithm", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, No. 2, 2007, pp. 214-223
[7] D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D. Culibrk, and B. Furht, "A Permutation-based Correlation- Preserving Encryption Method for Digital Videos," in International Conference on Image Analysis and Recognition, 2006,LNCS 4141,pp. 547-558.
[8] C. Bergeron and C. Lamy-Bergot, "Compliant Selective Encryption for H.264/AVC Video Streams," in Proceedings of the 7th IEEE Workshop on Multimedia Signal Processing ,2005, pp. 1–4.
[9] T. Lookabaugh, D. C. Sicker, D. M. Keaton, W. Y. Guo and I. Vedula, "Security Analysis of Selectively Encrypted MPEG-2 Streams," Multimedia Systems and Applications VI Conference, Orlando, FL, September 7-11, 2003.
[10] B. Bhargava, C. Shi, and Y. Wang, "MPEG Video Encryption Algorithms", August 2002, available at http://raidlab.cs.purdue.edu/papers/mm.ps
[11] X. Liu and A.M. Eskicioglu "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions," IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), Scottsdale, AZ, November 17-19, 2003.
[12] T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of Video Encryption Algorithms," Proceedings of The 3rd Central European Conference on Cryptology, TATRACRYPT 2003, Bratislava, Slovak Republic, 2003.
[13] C++ Implementation of AES by Szymon Stefanek Availableat: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
[14] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .
[15]Chandramouli, R., Kharrazi, M. & Memon, N., "ImageSteganography and steganalysis: Concepts and Practice",Proceedings of the 2nd International Workshop on DigitalWatermarking, October 2002
[16] BRASSIL, J. – LOW, S. – MAXEMCHUK, N. F. –O'GORMAN, L., Hiding Information inDocument Images, AT&T Bell Laboratories, Murray Hill, NJ.
[17] KUNDUR, D. – HATZINAKOS, D., Mismatching Perceptual Models for EffectiveWatermarking in the Presence of Compression, Department of Electrical and Computer Engineering University of Toronto 10 King's College Road Toronto, Ontario Canada M5S 3G4.
[18] Chandramouli, R. and N. Memon, 2001. Analysis of LSB based image steganography techniques. Proc. of ICIP, Thessaloniki, Greece.
[19] Robert Tinsley, Steganography and JPEG Compression, Final Year Project Report, University of Warwick, 1996
[20] Shi C, Wang SY, Bhargava B. MPEG video encryption in real-time using secret key cryptography. International conference on parallel and distributed processing techniques and applications (PDPTA'99), Las Vegas, NV, USA; June, 1999. p. 2822–8.

Siddharth Tiwari : was born in Jabalpur, MP India in 1987. He has completed his B.E. degree in Computer Science of engineering from Shri Ram Institute of Technology RGPV(Bhopal) MP, India in 2009.He is pursuing M.Tech in Computer Technology and Application at Gyan Ganga Collage of Technology Jabalpur (MP).He is the Oracle Certified Programmer of java technology. He is a life member of Computer Society of India. His area of interest includes Data Structure, Algorithms, Theory of Computation, Complier Design and Discrete Mathematics. He has Published two papers in national Conferences.

Prashant Kumar Koshta: was born in Jabalpur, MP India in 1980. He has completed his B.E. degree in Computer Science of engineering from Jabalpur Engineering Collage RGPV(Bhopal) MP, India in 2005. He is pursuing M.Tech in Computer Technology and Application at Gyan Ganga Collage of Technology Jabalpur (MP).He is a life member of Computer Society of India. His area of interest includes Data Structure, Algorithms, Complier Design and Computer Network and Data Communication. He has published four papers in national Conferences.