Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-19

# A Hybrid Approach for Enhancing Data Security by Combining Encryption and Steganography

Ashwini B, Pushpalatha S, R H Goudar
Department of Computer Network Engineering, VTU, Belgaum.

***Abstract*— In this era of fast growing technologies more attention needs to be paid for Security of multimedia data transferred over internet .Now a day's every one depends on the internet for data, so confidential data needs protection from third party. This can be achieved by using Cryptography, Compression and Steganography, all three together. These methods individually provide part of security so, when they are combined together, multi-level security can be provided. In the existing system, DCT is used for compression purpose which provides lossy compression and block cipher methods are used for encryption of secret data. Although these approaches are relatively secure, but high processing is required, it involves computational overheads and processing speed is less. Hence there are various techniques proposed by authors to provide security of the data, In our proposed system a hybrid approach of Compression, Double-Encryption and Steganography is employed to increase encryption speed, reduce processing time and also provides more security, authentication, authorization, Integration of data and also maintains confidentiality.**

***Keywords*-Cryptography, Steganography, Compression, chaotic mapping, LSB embedding,RSA.**

## I. INTRODUCTION

Over increasing security threats of multimedia data transmission over broadband Internet communication, lead to the encouragement of hybrid approach that involves Cryptography, steganography and Compression. These are the unique methods of providing Security, Integrity, and Authentication of confidential data.Above three methods are used for providing security individually, so when these methods are combined and applied security can be enhanced at higher rate. Cryptography(C), steganography(S) and compression (Com),as per our best knowledge several authors have proposed based on Com->C->S,C->Com->S combinations. So in our proposed system compression of data is done then it is encrypted, the keys used for encryption are also encrypted and then embedded in video .So, it becomes difficult for other than intended receiver to know about data and even if the data is extracted, because of the two Cryptographic methods used are unbreakable and more secured .There are several observations made for experimental purpose:

i) Image /video file formats.
ii) a. Compression->Encryption
b. Encryption->Compression

i) Image/Video file formats: The file format is the structure of encoding the data in computer file.

Image file formats: Here we consider three image formats and the comparison among them. The image formats are: Bmp, Png,gif, jpeg. Table 1 shows the comparison of file sizes when png,,bmp,gif formats are converted to jpg format. Table 2 shows the conversion of jpg file format to bmp,gif and png file formats and their respective sizes.

Table 1:

| | |
|---|---|
| Png file 99.5KB | Jpg file 10.8KB |
| Gif file 30.2KB | Jpg file 10.8KB |
| Bmp file 147KB | Jpg file 10.8KB |

Table 2:

| Jpg file | BMP file | Gif file | Png |
|---|---|---|---|
| 8.03 KB | 147KB | 30.2KB | 99.5KB |

Video file formats: Videos are the Sequence of images with certain amount of motion.

Videos are chosen for steganography, because more data can be embedded in the video than the single image and the

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-19

observed distortion is also less. Here we have chosen three video formats they are Mp4, flv, avi.

As all these formats are comparatively popular than other video formats. There are several softwares that make conversion among video formats; it does not affect quality of video only size will have variation.

ii) a. Compression->Encryption: If compression is applied first and then encryption is done then the size of data would increase again. This leaves less cleaves.

b. Encryption->Compression: If encryption is done first followed by compression then the size does not increase. This leaves more cleaves.

The system is organized into following sections: Section 2 covers Literature review, Section 3 covers Proposed system with the methods used, Section 4 covers Experimental Results, Section 5 Conclusion.

# II LITERATURE REVIEW

In this paper H.K.verma,et.al., [1] proposed Hybrid approach for increasing the security of the images. It provides secret and secure communication between respective parties and the performance is measured in terms of PSNR and MSE to check the effectiveness of proposed method. In this paper D.Rawat ,et.al.,[2]they have proposed improved LSB method for 24-bit image that provides stego-images that are indistinguishable from original images. Hence there is no loss of information during extraction and secret data is not disturbed. In this Paper K.Challita,et.al.,[3] have proposed new direction of enhancing security of secret data by using both cryptography and steganography. So that it becomes difficult for steganalysts to extract secret data. In this paper M.Vladutiu.et.al.,[4] proposed two state method of cryptography algorithm along with developing steganographic based secured system in order to enhance security issues of secret data communication. Hence integrity, authenticity and security of secret data as well as cover image also attained at higher rate. In this paper Yosua Kristinato.et.al.,[5] proposed the steganographic software that enhance security and confidentiality of hidden information and also provides an lenience for data exchange between intended sender and receiver .This method also avoids suspicion from third party on the communication between exchangers. In this paper Spyros S, et.al, [6] proposed the new approaches for digital video encryption; their advantages and classification of digital video encryption algorithms to elucidate (clarify) the advantages. Here encryption is performed after compression and decrypted before decompression; it is exclusive and popular feature. In this paper H.S.kwok,et.al.,[7] proposed the chaotic based encryption method with stream cipher,where PRKG(Psedo Random Keystream Generator) is used that is combination of 2 chaotic maps. Here encryption speed is increased and security is enhanced.

As per above papers referred, various authors tries to propose and implement security providing methods but no information or work is available on the proposed method as per our best Knowledge. Hence the three methods such as Cryptography, Steganography and Compression are combined in different sequence to develop stand-alone method for enhancing security of secret data over communication.

# III PROPOSED SYSTEM

In the Proposed System the methods of enhancing security are combined in different pattern so that the security is provided in multiple levels. The architecture of system provides sequential flow of system processes as shown in Fig 1 below.

At sender: Sender takes an image (Secret image) and it is compressed by compression Technique such as Discrete Wavelet Transformer (DWT), it provides lossless compression.

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-19

Then the compressed image is encrypted by chaotic mapping and the keys used here are encrypted with RSA algorithm so that Cryptography applied here becomes strong.

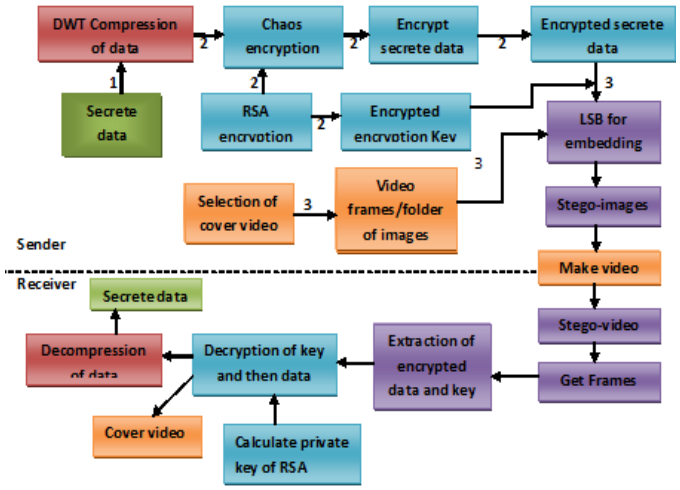



Fig 1. Architecture of Proposed System

The encrypted image is embedded in cover video by LSB embedding method, LSB method here is the LSB substitution so the video size after embedding image will not be changed. Then the cover video containing secret data along with encrypted key is accessed by intended receiver.

At Receiver: Receiver initially extract the encrypted image from stego-video and then generate Private key to decrypt the keys of chaotic mapping, then these keys are used to decrypt the encrypted image, then decrypted image is decompressed to original image or secret data that was encrypted and embedded in video.

Here both Symmetric and asymmetric encryption methods are used. Symmetric encryption is used for encryption of secret data and Asymmetric encryption is used for encryption of secret key that is used for encrypting data.

1. Discrete Wavelet Transformer (DWT):

Wavelet compression is subset of "transform-based compression". It involves lossless mathematical transform in order to provide a sparse representation of input image; the transform domains are then quantized to achieve desired level of compression. These quantized values are never restored to their original accuracy, but such quantization is necessary to achieve higher compression ratio.

2. Chaotic Encryption Method:

Choas based cryptography relied on complex dynamics of non-linear systems or maps that are deterministic but simple. Choas has special properties such as sensitivity depends on the initial conditions and system parameters, Ergodicity,quesi-randomness. These Properties make chaotic cryptography as an alternative to conventional cryptography methods. Conventional methods are based on discrete mathematics and take more processing time. chaos is faster and secure encryption method for multimedia data over broadband internet communication. General chaos based image encryption is shown in Fig 2.

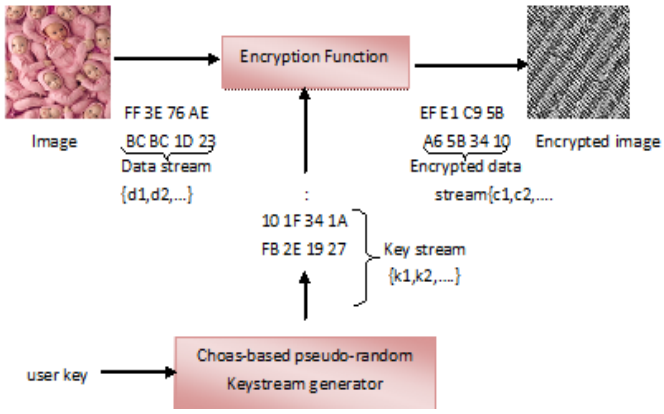



Fig 2.Chaos based encryption

Image is initially converted to binary data stream, by masking the data with random key stream generated by chaos based Pseudo-Random Keystream Generator (PRKG), and then resultant encrypted image is formed. This approach is light-weighted and has good performance.

Here Henon Chaotic maps are used specifically. It can be described by following.

$$x_{i+1} = 1 - a x_i^2 + y_i$$

$$y_{i+1} = b x_i, i = 0,1,2\ldots.$$

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-19

The above two equations have keys a&b, that are manually given by sender. The Henon map presents simple two dimensional map with quadratic non-linearity. It gives the first example of strange attractor with fractal structure, this map is simple, provides more shuffling of pixels. There are two keys that are used for encryption of secret data. The system is said to be chaotic with considered values a=0.3 and b=1.4 is shown in fig 3,this is usefull for encryption of image.

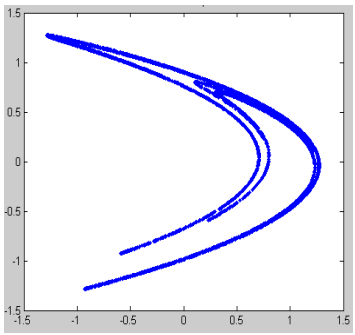


Fig 3:Chaotic behavior of Henon system

RSA Encryption: It is an Asymmetric encryption method, where public key and private key are used for encryption and decryption. Here we introduced RSA for encryption of secret key chaotic mapping method .The key is encrypted by public key at sender side and it is decrypted with private key.RSA provides higher security because the calculations involved are complex.

3. LSB Substitution:

This is the steganographic method used for embeddeding secret images in video in order to provide security for it. Here LSB bits of video i.e., Video is sequence of images so ,the LSB bits of each image are replaced by secret image bits .This provides less distortion of video as only LSB bits are replaced. The size of video is also not altered as there is bit substitution.

# IV EXPERIMENTAL RESULTS

In the proposed system Hybrid approach is employed for enhancing security, the algorithms used here are analyzed and implemented on matlab R2008,the performance is measured on Intel core,32 bit system with 500GB RAM running on windows 7 ultimate. Here images are used for analyzing .Fig 3 shows the subplots of (a) secret image(300×315) ,(b) encrypted secret image, (c) cover image before hiding (512×512) and(d) cover image after hiding. Peak Signal to Noise Ratio(PSNR) and Mean Square Error(MSE) both are the measuring parameters.

Both the cover images cannot be differentiated visually so, histograms are used to identify it .the respective histograms are shown in Fig 4.Image quality can be measured in terms of Peak signal to noise ratio of original image and recovered image. The reconstructed image is said to have high quality if the PSNR value is high. PSNR can be calculated mathematically as follows

$$\text{PSNR}=10\log_{10}\frac{\text{MAX}_\text{I}\,\hat{}\,2}{\text{MSE}}\ \text{(dB)}$$

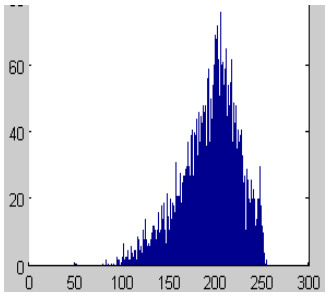
$$MSE = (1 \div mn)\sum_{i=1}^{MN}(Oi - ri)^2$$

Where, Oi and ri represents Original and reconstructed image pixels are by respectively. m*n represents the size of image.

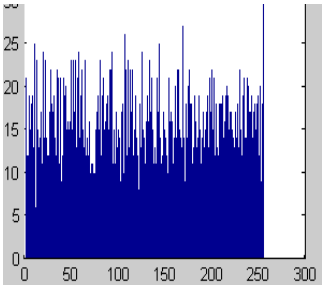
As the PSNR value reaches infinity the two images are said to be identical.

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-19

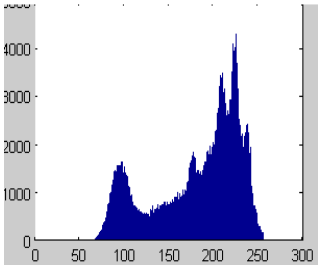
Fig 3. (a) secret image,(b) encrypted secret image,(c)Cover image before hiding/embedding,(d) Cover image after hiding/embedding.



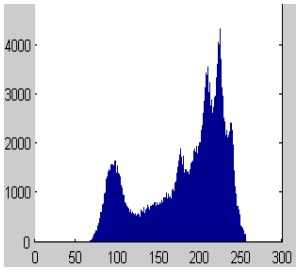
(a) Secret image



(b) Encrypted secret image



(c) Covering before Stego



(d) covering after stego

Fig 4. Histograms of: (a)secret image,(b) encrypted secret image,(c)Cover image before hiding/embedding,(d) Cover image after hiding/embedding.

# V CONCLUSION

The proposed system ensures integrity of secret data, with double encryption i.e., encrypting the data as well as encrypting the encryption key and video embedding is chosen so that large amount of confidential data can be embedded in it with less distortion, hence multilevel assured security with higher encryption speed and lesser processing is achieved and also experimental results assure that the quality and integrity of confidential data is attained over internet.

## *REFERENCES*

[1] Jaspal kaur saini, Harsh K verma,"A Hybrid approach for image security bycombining encryption and steganography",Proceedings of the 2013 IEEE second international conference on imae information Processing(ICIIP-2013).

[2] Deepesh Rawat,vijaya Bhandari,"A Steganography Technique for Hiding image in an Image using LSB method for 24 bit color Image",International journal of computer Applications(0975-8887)Volume64-No.20,February 2013.

[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(ISSN2220-9085).

[4] Mircea Vla dutiu and Lucian Prodan,"Secret data communication system using Steganography,AES and RSA",2011 IEEE 17th international Symposium for Design and Technology in Electronic Packaing(SITIME).

[5] Nur Hadisukmana,Yosua Kristinato,"Steganograpy software with combination of Encryption Algorithms for Multimedia files",2011 first International conference on Informatics and computational Intelligence.

[6] Daniel Socek.Hari Kalva.Spyros S.Magliveras,"New approaches to Encryption and steganography for digital videos",Multimedia Systems DOI 10 1007/s00530-007-0083-z,Springer-Verlag2007.

[7] H.S. kwok, Wallace K.S. Tang ."A fast image encryption system based on chaotic maps with finite precision representation", Department of Electronics Engineering. chos, solutions and Frctals 32(2007)1518-1529.www.elsevier.com/locate/chaos.

[8] Abdul Razzaque & Nileshsingh V.Thakut,"An Approach to Image compression and encryption",International Journal of image Processing and vision sciences ISSN (print):2278-1110,Volume-1,Issue-2,2012.

[9] A.J.Mozo,M.E.Obien,C.J.Rigor,D.F.Rayel,K.Chua,G.Tangonan," Video steganography using Flash Video", 12MTC International instrumentation and Measurement Technology Conference Singapore IEEE.

[10] Mazen AbuZaher,"Modified Least Significant Bit(MLSB)",Albalqa,Applied University,Amman,Jordan.Vol 4,No.1;January 2011.www.ccsenet.org/cis.

[11] Ramakrishna Mathe,Veera RaghavaRao Atukuri,Dr.Srinivasa Kumar Devireddy,Securing Information:Cryptography and Steganography,International Journal of Computer Science and Information Technologies(IJCSIT),Vol 3(3),2012,4251-4255.