Multilevel Information Security For Multimedia Data Communication

Amrutha H V, Anupama K, H P Chethana,
Kini Swati Satish
8thsem B.E, Dept. of CS&E, JNNCE,Shivamogga,
Karnataka,India.

Dr. R Sanjeev Kunte
Professor, Dept. of CS&E, JNNCE, Shivamogga,
Karnataka,India.

***Abstract*— In the present day, the information technology has become the most evolving technologies in the world. Multimedia is the content that uses a combination of different content forms such as text, audio, images, videos and also animations for the purpose of communication. Since the multimedia communication has increased enormously, which may be carrying the important data in it, information security becomes the utter need. Thus, three different level of security is provided based on the secrecy of the data to be communicated. Some simple but essential data can be sent with single level of security using steganography techniques. And for second level, steganography is used along with the encryption. And when highly sensitive and very important data needs to be communicated between two parties, then hashing and cryptography techniques along with steganography technique is used. Thus efficient security system can be built for any kind of data.**

Keywords- Steganography, Encryption, hashing, LSB technique, SHA.

I. INTRODUCTION

In today's world, secure information communication is major concern. Confidentiality of any kind of data communicated between two ends is very important. So if the data is allowed to send directly to the other end, then there can be threat of attacks from the intruders. Hence the various data security methods can help to overcome this problem.

There are different types of techniques available under the domain of the information security including Cryptography techniques, Hashing and Steganography techniques, and also the watermarking and digital signature techniques. Many other techniques have been evolved under the information security to provide the safest data transmission.

Steganography is the practice of hiding the data behind the carrier file such as image, audio, video [1][2][4]etc. Steganography involves combination of two words 'steganos' meaning covered and 'graphein' means writing. The main advantage of this technique is that the intended secret message does not attract the attention to itself as an object of scrutiny compared to other techniques. Steganography is the process in which generally some secret message is embedded into an innocuous looking simple image (called as the cover image) and creates a Stego image. The Stego image visually seems to be indifferent from the original cover but hides the secret message inside it and is transmitted to the desired recipients over the communication channels without creating any suspicion in the minds of the intermediately sniffers or/and receivers. When the authorized recipient receives the image, they follow the extraction procedure to retrieve the secret message.

Cryptography is the process of encoding a message, so that only authorized person can receive it safely[5][6][8]. Encryption is the process that produces a cipher text for any given plaintext and encryption key. Decryption is the process which produces a unique plaintext for any given cipher text and decryption key. Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out and they are, Symmetric Key Encryption and Asymmetric Key Encryption. The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption.

Hashing is used to condense a message into an irreversible fixed length value[8][10]. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by the hash functions are called as hash values or simply hashes. The hash functions are often used in combination with a hash table, a common data structure used in computer software for rapid data lookup. The idea of a hash code acting as a message "fingerprint" is reasonable, because making even the smallest change in the message data changes the value of the final hash code. Thus it can be used in managing the integrity of the data.

Thus in this paper, there is the implementation of data security of different levels using various information security techniques as mentioned above. If the data demand only single level security then steganography technique is used, and for double layered security, combination of both cryptography and steganography technique is used. If multilevel security is the demand, then the implementation of steganography is accompanied by both the encryption and hash based techniques for highest efficiency in data security. Thus provides the better security possible.

Rest of the paper is organized as follows. Related work on the multimedia data security is presented in section II, the proposed work with system architecture is given in section III. Experimental results and analysis are presented in section IV and conclusion in section V.

II. LITERATURE SURVEY

Poonam Yadav and Maitreyee Dutta [1] presented paper on 3-Level Security Based Spectrum Image Steganography with Enhanced Peak Signal to Noise Ratio.

The three levels of security have been designed as, first level security is provided by RSA Encryption with Diffie Hellman Key exchange algorithm. Second level of security is maintained by compressing the data to be hidden using Runlength Encoding and third level communication is more secure during pseudo random generator that generates random locations of pixels in an image.

Rini Indrayani [10] et. al proposed an approach to exchange data by combining steganography and cryptography techniques where the hidden data in cover file is encrypted using AES encryption and the key for encryption is encoded using MD5 hash function. The cover media used is mp3 audio file and the secret message file could be text, image, audio, video or compressed file.

Rinu Tresa M J [2] et. al depicted a process that combines both steganography and cryptography, along with hashing. The textual data entered by the user is encrypted using AES(Advanced Encryption Standard) algorithm after which, data is divided into blocks and stored in one array list and another array list will contain the pixel locations where these blocks has to be stored, obtained using a hash algorithm.

Ankit Chaudhary and Jaldeep Vasavada [4] proposed a Hash based Approach for Secure Keyless Image Steganography in Lossless RGB Images. The security level is increased by randomly distributing the text message over entire image and improves the storage capacity by compression techniques. The message to be hidden is first compressed and stored in the cover file using MSB bit of RGB channels as pixel indicator. The randomization is based on hashing with respect to MSB of channels to skip R number of bytes, where R is generated from Random Number Algorithm.

Gotfried C. Prasetyadi [3] et. al takes an input message which is a computer file of any type and hides in selected cover or carrier file which is a computer file of certain type. A special block of bytes called Identification (ID) block of 64 bytes is needed which contains a hash value, extension of file and a key index to point to start of message sequence in stego file. Advanced Encryption Standard (AES) with Rijndael Algorithm is used for encrypting the message with key length of 256 bits and message block size of 128 bits. A randomly generated 128-bit salt along with user given passphrase, is used to generate 256-bit secret key. The message is put into block of 128 bit using PKCS7 padding.

Siva Shankar S and Rengarajan Alwar [5] presents a novel data hiding and image encryption scheme using random diffusion and two-dimension Arnold cat mapping transform. The secret message bits are placed in lsb positions of cover image. The shared key is used to generate 8-bit random integer stream and is added to stego image in random diffusion step. Arnold cat transformation is done to scramble the pixels. Two step random diffusion and Arnold transform mapping are done alternatively several times to completely encrypt the image content. Pseudo random generator is setup with shared key.

Anil Kumar and Rohini Sharma [9] proposes a technique to transmit the data securely by combining cryptography and steganography. This technique applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. This technique enhances the LSB technique to hash LSB technique. The secret message is encrypted using RSA algorithm. Then the four least significant bits of each RGB pixel are chosen from the cover image. The hash function is applied on LSB to get the position. Then the eight bits of the encrypted message are embedded into the four bits of LSB in the order of 3, 3 and 2 respectively. The resultant stego file is transmitted.

Shreyank N Gowda [11] uses least significant bit of each pixel and information is hidden in that. First the data is encrypted using the Blowfish algorithm. This encrypted block is broken down to 'n' smaller blocks and 'n' images are chosen at random and each image is made to hide a block of the encrypted data. To maintain the correct sequence of blocks a hash table is maintained. This is then encrypted using LSB to a new image called the hashing image. This hashing image is sent along with the 'n' other images. To extract the data out, first the hash image is obtained and using this the encrypted block is reassembled and then original data is obtained by decryption.

III. PROPOSED WORK

In the proposed system, the data security is given the utmost importance. This system provides multilevel security as required for communicating confidential data securely between two parties. Depending upon the level of security needed for different application, some of the techniques like, steganography, cryptography and hashing are used to provide multilevel security for multimedia application.

System Architecture

The block diagram of the system architecture is shown in Fig 1 and Fig 2. The sender and the receiver side security architecture is provided separately in these two figures.

A. Sender side

- The application user (sender) has to select the level of security that he wishes to provide for his data.
- If the user wishes to provide simple security to the data, he can select choice 1. Under this choice, steganography technique is applied. The secret data to be transferred is hidden within a cover file and transmitted over the network.
- If the security for the data required is two level, select choice 2. Under this choice, cryptography and steganography techniques are applied on the data. The secret message is first encrypted. This encrypted message is embedded into the cover file to provide the second layer of security. The resultant stego- file is transmitted to the receiver.
- If the data is highly confidential, then select choice 3. Under this choice, three techniques viz. cryptography, steganography and hashing are combined to provide security. Initially, the secret data is encrypted. Also, the hash of the original message is calculated. The calculated hash value is appended to the encrypted data. The outcome is transmitted to steganography unit where the data will be embedded within the cover file and transmitted over the network.

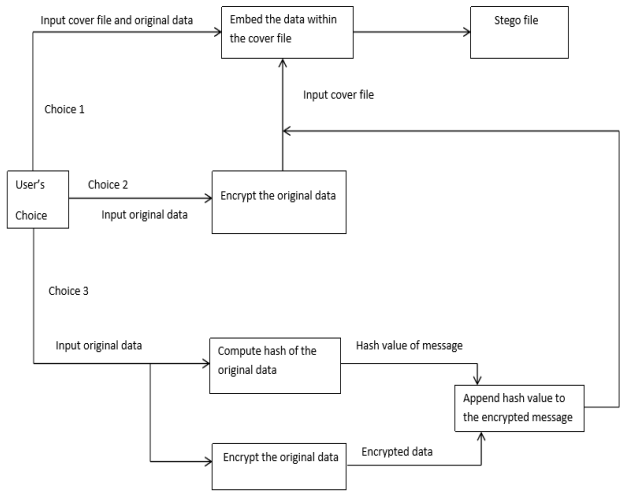

Fig 1. Block Diagram for the multilevel security at sender.

A. *At Receiver side*

- The user (receiver) has to extract the message received. The message retrieval process depends on the level of security that the sender has provided to his data.
- If the sender has transmitted the message with single level of security, then at the receiver end the original message will be extracted from the stego file using the reverse of the technique used at the sender.
- If the sender has transmitted the message with two level security, then at the receiver end the encrypted message will be extracted from the stego file. Later, the decryption of the extracted message is carried out to obtain the original message.
- If the level of security provided by the sender is 3, at the receiver end, the hash appended encrypted message will be extracted from the stego file. Then the encrypted message will be decrypted. The decrypted plain text is used to calculate the hash value. The calculated hash value and the hash value transmitted by the sender are compared for equality which ensures the data integrity of the message.

a. Level 1: 3-3-2 LSB Steganography:

In this technique, the least significant bits of r, g, b pixels are used for hiding the secret message data [12].

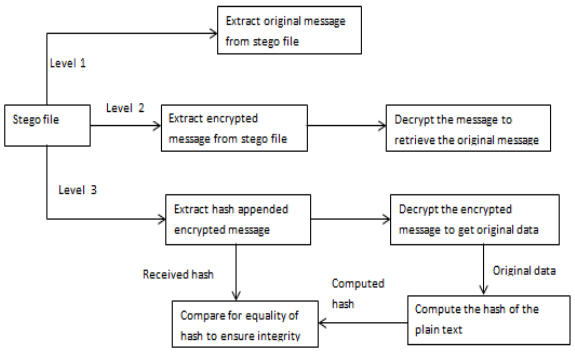

Fig 2. Block diagram for multilevel security at receiver.

Text as the secret data

For every character in the text data:

i. Convert the data to binary value.
ii. Select the random pixel value of the cover image within which the data has to be embedded [7].
iii. The 8 bits of the cover image is divided into 3-3-2 bits.
iv. Embed every 8 bits at last 3 bits of red, last three bits of green and last 2 bits of blue pixels selected randomly.

Image as the secret data

For every pixel of the secret image:

i. Convert the pixel value to 8 bits binary.
ii. Select the random pixel value of the cover image within which the data has to be embedded.
iii. The 8 bits of the cover image is divided into 3-3-2 bits.
iv. The first three bits of the secret image pixel are stored at the last three bits of red pixel of cover image.
v. The next three bits of the secret image pixel are stored at the last three bits of green pixel of cover image.
vi. The last two bits of the secret image pixel are stored at the last two bits of blue pixel of cover image.

The same technique can be applied for audio file.

b. LEVEL 2: Steganography and Cryptography:

In this level the 3-3-2 LSB steganography technique [7][12] and xor operation [6] for cryptography is used for increased security.

Following steps shows the level 2 implementation:

i. The technique used for cryptography is the xor operation [6].
ii. The key image is the random image that is generated.
iii. The data to be encrypted be it text, image, audio will be read.
iv. The key image having the same size as that of the secret data is generated using pseudorandom numbers.
v. The generated key image and the secret data are xored bitwise.
vi. The resultant value is the encrypted data.
vii. The encrypted data is further hidden inside a cover image using 3-3-2 LSB steganography technique.
viii. At the receiver end, the encrypted data embedded within the cover image is extracted and then decrypted to get the original data.

c. LEVEL 3: Steganography, Cryptography and Hashing:

In this level steganography (3-3-2 LSB technique), xor operation for cryptography and SHA-256 algorithm for hashing is used for the better security [8].

The following are steps for level 3 security:

i. The hash value of the original message is computed using the SHA- 256 algorithm [8].
ii. The computed hash value is embedded within the cover image.
iii. The original data is encrypted using the xor operation and the encrypted data is hidden within cover image using 3-3-2 LSB steganography.
iv. At the receiver, the encrypted data is extracted from the cover image and decrypted.
v. The hash value of the original data obtained at the receiver is computed using the SHA-256 algorithm.
vi. The received hash value and the computed hash value are compared and if they are same, then the integrity of the data is ensured.

IV. Experimental Results

The proposed method has been experimented for different size and type of secret data. The standard images such as *Baboon*, *Lena*, *Pepper*, *Cameraman* can be used as the cover image for hiding secret data which may be text file, image or audio. The proposed system is tested for all three levels of security. Fig. 3 and Fig. 4 show the snapshots of experiment conducted for image file at level 1 where the secret image is standard *Pepper* image and the cover image is *Baboon* image. At level 2, cryptography is applied before hiding secret data. Fig. 5 depicts the result of applying xor operation to image file where *Lena* is the secret image. The proposed system is also tested at level 3, which is the combination of hash, cryptography and steganography.

The performance is measured by computing the Mean Square Error (MSE) and Peak Signal to Noise ratio (PSNR) value for stego image and cover image.

Fig.3 Cover image before and after hiding secret image at level 1.

Fig.4 Secret image before and after extracting at level 1.

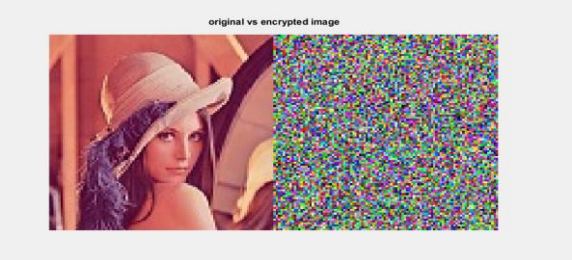

Fig 5. Secret image before and after xor operation with randomly generated image at level 2.

If I of size m x n is the original image and K is the encrypted image then MSE is given by:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad \ldots\ldots\ (1)$$

The PSNR is given by the following equation.

$$PSNR = 20.\log 10\left(\frac{MAXf}{\sqrt{MSE}}\right) \quad \ldots\ldots\ (2)$$

Where MAXf is the greatest conceivable pixel estimation of the image, at the point when the pixels are written by utilizing 8 bits for each pixel, this is 255.

For steganography the MSE value should be less and PSNR value should be high. The Table 1 shows the performance analysis for steganography. The cover image (*Baboon*) is of constant size of 250x250 resolution. The size of secret image (*Pepper*) is varied as shown in Table 1 and the values for MSE, PSNR, time to create the stego image.

Table 1. Performance analysis for steganography

HIDING PIXEL AS (3,3,2) BIT POSITIONS	COVER IMAGE (SIZE)	SECRETIMAGE (SIZE) (colour image)	PSNR (Db)	MSE	TIME TO HIDE (SEC)	TIME TO EXTRACT (SEC)
1	250*250	20*20	56.8264	0.1350	0.2508	0.1877
2	250*250	50*50	48.6281	0.8918	1.2691	0.9819
3	250*250	100*100	42.6205	3.5565	4.8831	3.4065
4	250*250	140*140	39.6709	7.0144	9.4236	6.6943

The results show that PSNR value is more than 40 dB. This shows that the embedded secret image is imperceptible and do not degrade the quality of the cover image.

For encryption the MSE value should be more and PSNR value should be low. The table 2 shows performance analysis for cryptography. The standard Lena.png is xored with a randomly generated image and this is done for different sizes to compare the values of MSE and PSNR, time taken for encryption and decryption and the entropy.

Table 2. Performance analysis for cryptography

MESSAGE TYPE	XORED WITH	ENCRYPTION TIME (in seconds)	DECRYPTION TIME (in seconds)	MSE	PSNR (db)	ENTROPY
Lena.png	Random Image (10x10)	0.6275	0.1972	7.8250e+03	9.1960	6.1337
	Random Image (50x50)	0.6962	0.1850	8.7074e+03	8.7319	7.5607
	Random Image (150x150)	0.6344	0.1685	8.8360e+03	8.6683	7.6150

Table 2 shows that the value of MSE is very high and that of PSNR is low which is as needed for cryptography. The value of entropy is reasonably good and the time taken to encrypt and decrypt the secret data is less than a second.

V. CONCLUSION

The data security method developed in this paper provides security using three different levels. Data is embedded using steganography technique. At further levels, the encryption is used along with level one. Additionally for highest security, hashing is used at level three. Thus this increases the security for data communicated. The developed system exhibits high PSNR and low MSE values indicating that the system has good imperceptibility property.

REFERENCES

[1] Poonam Yadav, Maitreyee Dutta. "3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio." In Image Information Processing (ICIIP), IEEE, pages.1-5, 2017.

[2] Rinu Tresa M J, Athira M Babu, Sobha T: “A Novel Steganographic Scheme Based on Hash Function Coupled with AES Encryption”, at Advanced Computing: An International Journal(ACIJ), Vol.5, No.1, pages.25, 2014.

[3] Gotfried C. Prasetyadi, Achmad Benny Mutiara, Rina Refianti: “File Encryption and Hiding Application based on Advanced Encryption Standard(AES) and Append Insertion Steganography Method”, In Informatics and Computing (ICIC), IEEE, pages.1-5, 2017.

[4] Ankit Chaudhary, Jaldeep Vasavada: “A Hash based Approach for Secure Keyless Image Steganography in Lossless RGB Images”, In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), IEEE, pages. 941-944, 2012.

[5] Siva Shankar S, Rengarajan Alwar: “Data Hiding in Encrypted Images using Arnold Transform”, in ICTACT Journal on Image and Video Processing, Vol.07, No.1, pages.1339-1344, 2016.

[6] Yani Parti Astuti, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari: “Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB”, in International Conference on Information and Communications Technology(ICOIACT), 2018.

[7] Sunny Dagar: “Highly Randomized Image Steganography using Secret Keys”, In Recent Advances and Innovations in Engineering (ICRAIE), IEEE, pages.1-5, 2014.

[8] Chetna Mehto, Rachana Kamble, Dr. Bhupesh Gour: “An Enhanced Digital Text Passing System using SHA-512 and AES”, Computer Engineering and Intelligent Systems ISSN 2222-1719(Paper) ISSN 2222-2863(Online), Vol.6, No.7, pages.35-43, 2015.

[9] Anil Kumar, Rohini Sharma: “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol.3, No.7, 2013.

[10] Rini Indrayani, Hanung Adi Nugroho, Risanuri Hidayat, Irfan Pratama: “Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function”, In Science and Technology-Computer (ICST), IEEE, pages.129-132, 2016.

[11] Shreyank N Gowda: “Using Blowfish Encryption to Enhance Security Feature of an Image” at sixth International Conference on Information Communication and Management, IEEE, pages.126-129, 2016.

[12] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara: “Data Security Using Cryptography and Steganography Techniques”, at International Journal of Advanced Computer Science and Applications (IJACSA), Vol.7, No.6, pages.390-397, 2016.