Enhancing Image Security by employing Blowfish Algorithm further embedding text and Stitching the RGB components of a Host Image

Deepanshu Agarwal, Pravesh Panwar, Purva Vyas, T.B. Patil, S.D.Joshi

Abstract*: *'Privacy, privacy everywhere but not a safety method to implement it': a harsh reality of today's world. With the precipitation of more data (2 x 10^{19} bits of data is created in every 86400 seconds) in computer networks, involvement of meta-data in the form of images is essential. To keep data safe and secure in order to inculcate privacy, to eradicate any kind of eavesdropping, and to maintain confidentiality, integrity and availability of it, certain security measures are needed to make in account for. So in order to make it available, we required a technique through which we can securely transfer any kind of data over a network. In practise the information security can be achieved either by using Cryptography or Steganography.

The process described in this paper is not a mediocre it is more scrupulous towards the security because it involves image encryption, steganography and image stitching. Initially we are encrypting an image using Blowfish algorithm then we are embedding the secret text into this encrypted image by modifying the least significant bit (LSB) of the image by our data. Moreover, to enhance the privacy and security we are stitching the above resultant image with the red, green and blue (RGB) components of a host image and thereby producing an image more secure than the one which the existing systems can form for data transmission..

Index Terms*: *Blowfish Algorithm, Data Embedding, Feistel Network, Image Stitching, Steganography, Twofish Algorithm

I. INTRODUCTION

We live in the greatest human civilization ever developed or constructed by humans in which accessing data for survival becomes sine-qua-non. Yet, we are unaware of the malpractices conducted by intruders. These practices ignites because the deliveries to the recipients by the sender is no longer confidential, integrated and authenticated. With the inducement of computer networks where the multimedia was used literally in every ounce of information either in the form of text, image, audio, video and other multimedia types, providing security to such an element of information is critical and tedious. In the past decade Computer scientists from all over the globe have literally proposed plethora and pragmatic remedies to various problems in security and privacy that we as human accounts in our life. Since the percentage of integrated data on internet when compared to the data in multimedia form is zilch and hence providing abysmal security to this (multimedia) component won't be a good idea to entertain. To make the transmission of data more secure in this booming era of internet, where we have literally made the globe shrink to a size of our palms; we have successfully devised enormous encryption standards to prevent data transmissions from espionage in the past couple of decade. But the irony is that encryption was first used as early as 100 B.C. We have incorporated the practice of encryption a long time ago but we failed to "inculcate" within us and as a ramification even today we suffer from transmitting our data securely even though we are equipped with complex mathematical based formulae for encryption.

In this paper we are going to make the data, an image to be extreme precise, more efficient in terms of security via techniques like image encryption, steganography and image stitching. For, image encryption we are using Blowfish algorithmfurther we are embedding the secret text into this encrypted image by altering the least significant bit (LSB) of the image by our data. Moreover, to enhance the privacy and security we are stitching the above resultant image with the red, green and blue (RGB) components of a host image and thereby producing an image more secure than the one which the existing systems can form for data transmission.

II. LITERATURE SURVEY

Many algorithms have been incorporated for providing security for data transmission such as Advanced Encryption Standard (AES), blow-fish algorithm, two-fish algorithm, Data Encryption Standard (DES) and many others. But even with the existence of such algorithms we have not reached a par where a cent secure transmission for data could exists.

In this paper Blowfish is used to encrypt the image. Blowfish is a symmetric64-bit block, fiestel network cipher. It considers key length ranges from 32 to 448 bits.It is a fast and license-free alternative to existing encryption algorithms.Bruce Schneier is credited as one of the main person for the existance of both Blowfish and Twofish algorithm. Blowfish came into existence in 1993 whereas

Revised Version Manuscript Received on 16 September, 2019.

Deepanshu Agarwal, Information Technology, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.

Pravesh Panwar, Information Technology, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.

Purva Vyas, Information Technology, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.

T.B. Patil, Information Technology,Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India

S. D. Joshi, Computer Engineering,Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.

Twofish was developed in 1998 and Twofish can be considered as an enhanced version of Blowfish.

Twofish is a symmetric key (key sizes up to 256 bits) block (block size of 128 bits) cipher. Twofish's distinctive features are the use of pre-computed key-dependent S-boxex, and a relatively complex key schedule. Half of the key (n/2) is taken into consideration as an actual key for encryption and the residual i.e., n/2 key is used in S-boxes. Twofish borrows some elements from other designs; for example, the from the SAFER family of ciphers. Twofish has a Feistel structure like DES. Twofish also employs a maximum distance separable matrix. At the time of its designing the focus was to follow the NIST's rules for advance encryption standard.

Twofish specifics are as follows:

• It is efficient in both hardware and software platforms and does not include any hardware component or an element that reduces its efficiency. Hardware efficiency can be argued with the fact that it can be implemented with less than 2 x 10^4 logic gates.

• Flexible and simple design. Flexible in the sense that it supports large variety of range in key lengths up to 256 bits which can be implemented on various platforms and applications.

• It takes at max 500 clock cycles on Intel's Pentium architecture per block to encrypt data.

• For optimal speed of encryption the key length is set to 128-bits long in much lesser time than to encrypt 32 block on Pentium architecture.

• It supports only efficacy operations on any 8,16,32- bits micro processors and some 64-bit microprocessor.

• With respect to performance trade-offs many observable changes occurs with key scheduler.

• Generally on a 8-bit microprocessor it takes at most 10 milliseconds to encrypt the data.

• It requires only 64 bytes of RAM to rum on a 8-bit micro processor.

Twofish cryptographic goals were as follows:

• 16-round Twofish (without whitening) should have no chosen-plaintext attack requiring fewer than 280 chosen plaintexts and less than 2N time, where N is the key length.

• 12-round Twofish (without whitening) should have no related-key attack requiring fewer than 264 chosen plaintexts, and less than 2N/2 time, where N is the key length.

• Have variants with a variable number of rounds.

• Have a key schedule that can be precomputed for maximum speed, or computed on-the-fly for maximum agility and minimum memory requirements. Additionally, it should be suitable for dedicated hardware applications: e.g., no large tables.

• Be suitable as a stream cipher, one-way hash function, MAC, and pseudo-random number generator, using well-understood construction methods.

• Have a family-key variant to allow for different, non-interoperable, versions of the cipher. We feel we have met all of these goals in the design of Twofish.

The building blocks of Twofish algorithm are:

1. Feistel Networks

Any function can be transformed into sets of permutations using a general approach of a feistel network. Twofish is a 16-round Feistel network with a bijective function.The basic ingredient of a feistel network is a key dependent function which maps an input string to an output string, known as F-function. An F function is always non-linear and possibly non-surjective:

$$F : \{0,1\}^{n/2} \times \{0,1\}^{N} \rightarrow \{0,1\}^{n/2}$$

where,

n is the block size of the feistel network

N is the bits of the key; taken as input

F takes n/2 and N as input and generates a output string of length n/2. In each and every iteration of the round the source block, input to F, is xor-ed with the target blocks and the two blocks (source and target) are swapped and passed as input to the next round. Many iterations of the rounds makes the F function strong. A cycle is the termed used to define couple of rounds of a feistel network and in each and every cycle every bit of the text block is modified once.

2. S-boxes

An S-box is a table-driven non-linear substitution operation used in most block ciphers. The input and the output size of the S-box is dynamic in nature and thus it size varies also we can generate it either randomly or can be constructed using some algorithms. The first usage of a S-box dated back to the Lucifers. Two-fish empowers four various bijective and key dependent 8x8 boxes. These boxes can be constructed by using two fixed 8x8 permutations and the key.

3. Maximum Distance Separable (MDS)

The maximum distance separable code over the field 'a' and 'b' is a linear mapping of field 'a' elements to field 'b' elements, generating a+b as a composite vector of the elements, with the property that the minimum number of non-zero elements in any non-zero vector is at least b+1. The number of elements that are distinct is known as the 'distance'. So, in other words the distance between any two distinct vectors is at least b + 1. Since it is the maximum distance that can be achieved

here with any mappings, hence the term maximum distance separable. Maximum distance separable mappings can be visualized by a matrix of size a x b. Error correction codes of Reed Solomon are known as maximum distance separable. A necessary and sufficient condition for an a×b matrix to be MDS is that all possible square submatrices, obtained by discarding rows or columns, are non-singular. Twofish uses a single 4-by-4 MDS matrix over GF(28).

4. Pseudo-Hadamard Transforms

A pseudo-Hadamard transform is a simple software operation used for mixing. Given two inputs, a and b, the 32-bit PHT is defined as:

$$a' = a + b \bmod 232$$

SAFER uses 8-bit PHTs extensively for diffusion.

$$b' = a + 2b \bmod 232$$

Twofish uses a 32-bit PHT to mix the outputs from its two parallel 32-bit g functions. This PHT can be executed in two opcodes on most modern microprocessors, including the Pentium family.

5. Whitening

Whitening, the technique of xoring key material before the first round and after the last round, was used by Merkle in Khufu/Khafre, and independently invented by Rivest for DES-X [KR96]. In [KR96], it was how that whitening substantially increases the difficulty of key search attacks against the remainder of the cipher.In our attacks on reduced-round Twofish variants, we discovered that whitening substantially increased the difficulty of attacking the cipher, by hiding from an attacker the specific inputs to the first and last rounds' F functions. Twofish xor'es 128 bits of subkey before starting and ending of a feistel network. These subkeys are calculated in the same manner as the round subkeys, but are not used anywhere else in the cipher.

6. Key Schedule

A key can be transformed into the round keys, which a cipher uses by using a key schedule. Depending upon the requirement of a key in the algorithm the complexity of a key scheduler is varies. If the encrypting algorithm requires less key materials then a simple key scheduler can be designed but for algorithms like Twofish, which requires many materials of a key, a complex key scheduler is a must.

Steganography is a science of exchanging the information in a method that hides the existence of exchanging the information. Steganography in contrast to cryptography is an art to dodge the antagonist of the existence of the actual credential image by camouflaging with the host image. It is used for aggrandizing the security of the encrypted image which aims to cover-up the "secret" message into cover image, where the image is implanted with secret message so called stego-image. Steganography can be incorporated in many form and techniques but in this paper we concerns ourselves to shed light on using LSB(Least Significant Bit) substitution for Data Embedding over an encrypted image.

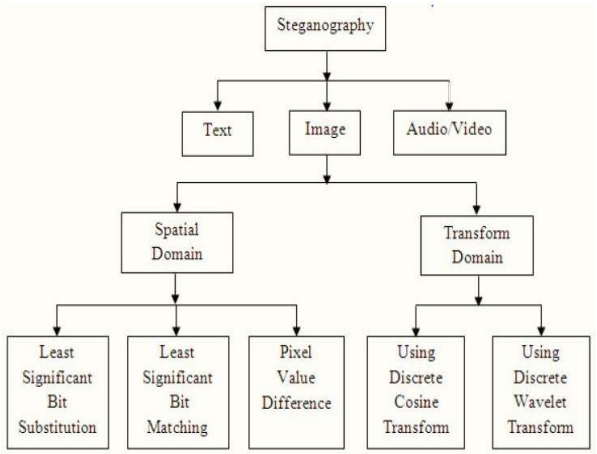


Figure 1: Classifications of Steganography

The Least Significant Bit is a technique which deals with hiding information that an intended user can easily understand and the data is hidden by replacing the LSB of each pixel by the secret text or message [4] which makes the Data Embedded techniques a very efficient and easy to use technique. LSB based data embedding over an encrypted image can be performed by extracting last bit of a pixel.

Now further we embed the encrypted image over a host image this is configured by using the last bit of every pixel which constitutes of red, green and blue (RGB) components. The other techniques which is used in RGB color model are:

- Least Significant Bits: This technique can be accomplished by using two approaches i.e. either each pixel of specific color channel is replaced with the cipher text or the secret data can be embedded by replacing the LSB of all the color channels. Since the data is added in the least significant bit the file size does not increase significantly. This technique is an example of spatial domain technique.
- Stegno Color Cycle: A regular-repeating pixel specific pattern is to be formed after employing this enhancement technique of LSB to the secret data. For instance the first bit of the secret data is stored in LSB of red channel, the second bit of the secret data in the green channel's LSB, the third bit of secret data in stored in the LSB of blue channel and so on
- Pixel Indicator: In this technique one of the available color channel is used as indicator and other two color channels will be used as container for secret message. It is a keyless steganography approach.
- Image Intensity: It suggests storing inconsistent number of bits in each channel of pixel based on the real color value of that pixel.

Moreover in this paper Image stitching is also used and it is defined as s a technique in which various portions of an image are wrapped together to form a single image [5]. In this approach first we divide the cover image with the ciphered image and the secret text embedded in it into multiple parts. Each part is then separately sent to the

recipient and at the recipient end the sub images are stitched back to regain the original image. The image obtained by applying above algorithms will be more secure to transmit and hence we are sending this image to the receiver where the decryption algorithm takes place to view the desired content.

III. IMPLEMENTED SYSTEM

The existing system present either work on an embedding of an image or data on a host image. The methods present for information and image hiding in a host image have some drawbacks like they either do not encrypt the image or use the weak algorithm to perform cryptography. The existing system also does not able to carry both the credential image and data to the receiver. The algorithm used by the system are not able to guarantee the security of an image and data breach been transmitted over the network so it is better if one goes for algorithm using keys of larger size which are difficult to decrypt and hence provides better security. The system which we have implemented is for secure image transmission over a network which can be seen as an integration of multiple system present. The proposed and developed system in this paper divided into three levels for better understanding, the levels are as follows:

- Image encryption phase
- Steganography phase
- Image stitching phase

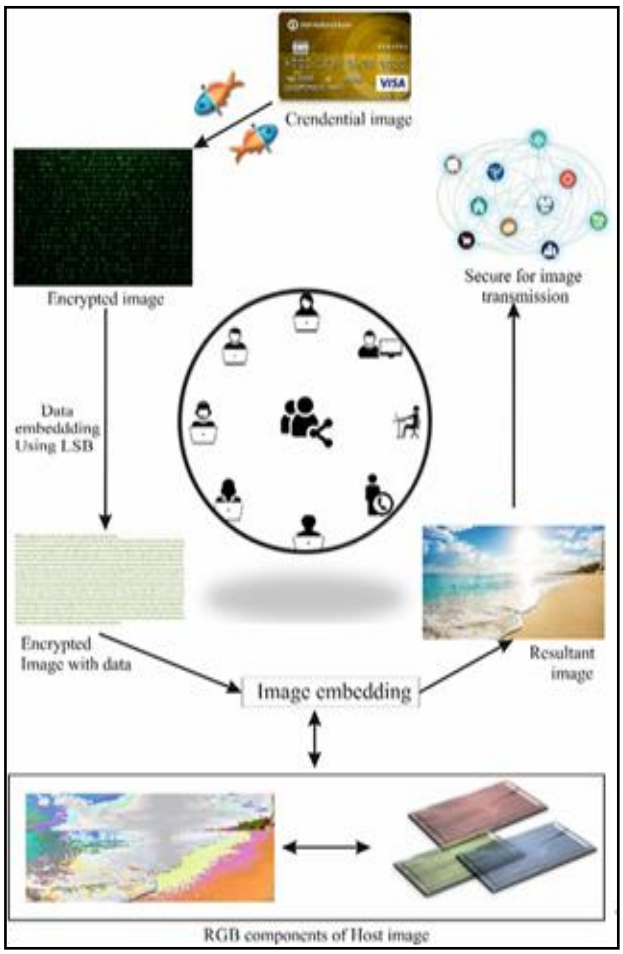


Figure 2: Architectural flow of the System

Image Encryption phase:

Blowfish is a symmetric64-bit block, feistel network cipher. It considers key length ranges from 32 to 448 bits.As shown in the figure Blowfish consists of two parts:

- Key expansion
- Data Encryption

The key expansion part makes sure that key length does not exists more than 448 bits. This part of the algorithm is also responsible to convert the key into several sub keys arrays totaling 4168 bytes.

To obtained the results from data encryption phase, 16-rounds of Feistel network happens. It is used in those applications where the key does not change It is often used in an automatic file encryption , communication links; where key does not change often. Initially, Blowfish was designed for a 32-bit microprocessors and in terms of speed it stands at pole in this segment.

As given in the figure the actual steps Blowfish algorithm follows in order to encrypt:

- X is 64 bitsinput data
- X is divided into two equal parts x1 and x2
- For i=0 to 15
  X1=x1 xor Pi
  X2=f(x1) xor x2
- Swap x1 and x2
- Swap x1 and x2(undo the previous step)
- X1=x2xor P18
- X2=x2 xorP17
- Combine x1 and x2

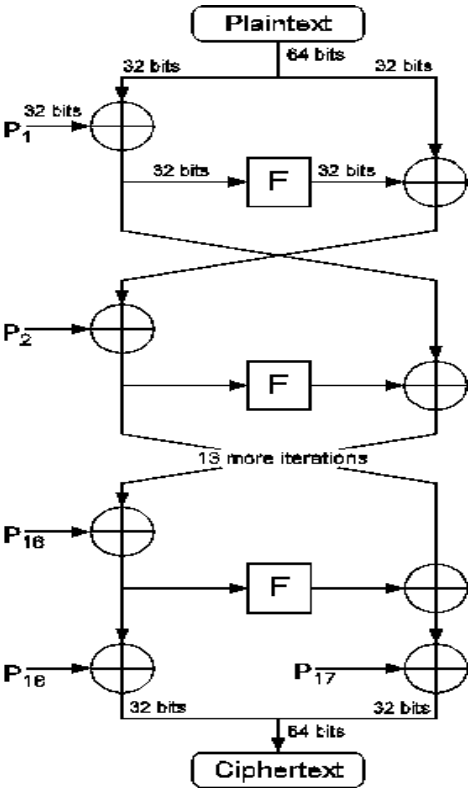


Figure 3: Blowfish Algorithm

When compared to texts images are bulky and hence Image encryption consumes a lot of CPU usage and thus it is a time consuming process. So, the factors which decides the approval of an algorithm for encryptions are speed and accuracy. The tables shows the statics of various encryption algorithms, the efficient algorithm can be selected depending upon the required security level of the application.

	Input Image Size (KB)	Encryption Time (s)	Decryption Time (s)	Execution Time (s)
Blow-Fish	388	0.82	0.69	1.51
	2441.41	4.45	4.41	8.86
	3818.359	7.40	7.41	14.81
	14062.5	27.32	27.36	54.68
Total	20710.269	39.99	39.87	79.86
Data Transfer Rate	20710.269/79.86 = 259.33 KB/s			

Table I: Data transfer rate of Blowfish

File	AES (ms)	DES (ms)	RSA (ms)	Blowfish (ms)
1 MB	102.6	161.3	481.5	156.4
2 MB	178.3	245	691.5	230
5 MB	206.8	356.8	1031.7	250
10 MB	294.6	480.4	1437.1	336.3
20 MB	406.5	669.3	1816	440.4

Table II: .Data table for Encryption runtime of Image Files

File	AES (ms)	DES (ms)	RSA (ms)	Blowfish (ms)
1 MB	159.8	175.2	4.1	65.5
2 MB	256.1	276.6	4.5	92.7
5 MB	311	400.8	4.7	123.8
10 MB	398.6	554.6	4.7	169.9
20 MB	485.4	696.9	4.7	218.5

Table III: .Data table for Decryption runtime of Image Files

Steganography Phase

The message is embedded on to a part of the encrypted image done by blowfish algorithm therefore credential data is given as input to the text editor. Hiding credential data text inside the cipher image is done using LSB steganography algorithm.

In an LSB algorithm:-

The three main colors are Red, Green and Blue. Each is 8 bits long and thus can have 256 (2^8) values. Since each pixel consist of equal proportions of RGB so each pixel can have as many as 2^{24} colors.

- Every pixel can have any of the 256 colors.
- Every pixel can have one in 256 shades of gray.

In this each bit of the credential data is exchanged with last bit of each pixel Value. Therefore four possibilities of swapping occurs i.e., replacing '0' with either '0' or '1' and similarly, replacing '1' either by '0' or by '1'.The LSB is changed only during the two cases out of four means whenever a '0' is replaced with a '1' and '1' is replaced with a '0' and hence drastic change is not visible because the absolute difference in the value of the resulting pixel and the original pixel is not much as a ramification the resultant image will resemble the original encrypted image. It must be noted that the end of the data must be represented by the NULL or special characters.

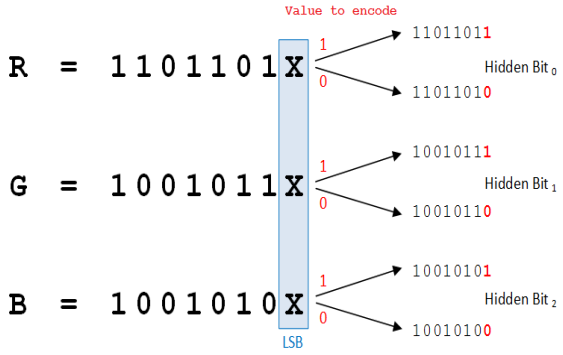


Figure 4: Example illustrating LSB

The efficiency and efficacy of steganography mostly depends upon the cover-image and stegno image. So, the major factors effecting stegnography are:

- Robustness: It refers to the ability of the secret data to maintain its latent state in the stegno image even if the image is undergoing transformations. The transformation can be linear and non-linear filtering, rotations and scaling, , addition of random noises, cropping or decimation, sharpening or blurring , lossy compression.
- Imperceptibility: It refers as the invisibility of a steganography algorithm to outside world.
- Bit Error Rate:It is defined as the ratio of the number of errors to the total no of bits sent in an image. This error populates at the time of retrieving the cipher text.

Image Stitching Phase

The smallest indivisible element of an image is termed as a pixel which means each and every pixel of an image acts like a sample of the original image. It means, more samples provide more accurate representations of the original. The intensity of each pixel is variable. The color imaging systems are:

i) RGB (red, green, blue)

ii) CMYK (cyan, magenta, yellow, black)

In this phase we use RGB components of a host image conceive our cipher image. We use the LSB technique which is used earlier in data embedding phase. With the help of changing the LSB bits of RGB componen399ts there is no significant change in quality and perceiving the image by the human eye. Hence the output produced by this phase is the resultant image which is safe and secure to transfer over a network without the fear of disclosing the confidentiality and authenticity of an image to leak.

IV. RESULT

The following are the screenshots of the projects. The various screenshots shows various stages of the project we implemented.

Step 1: Begin the process

The project's first user interface gives two option to the user. The user can either press 1 for encryption and 2 for decryption. Generally, the sender presses 1 and at the receiver's side option 2 is selected.

Step 2: Take the image for encryption

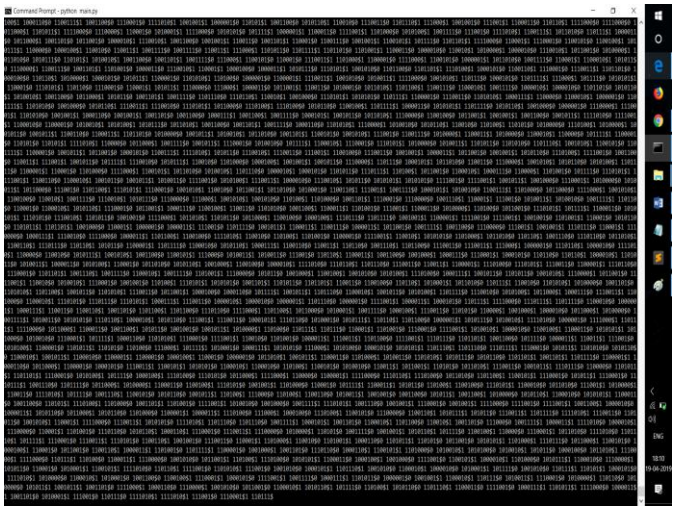
Next step is to select an image for encryption. The encryption algorithm used is Blow-fish, which is symmetric 256 block cipher. This image can be any credential image that the sender have to send to the receiver.

Step 3Apply the Blowfish Algorithm

Blowfish is a symmetric key, key length ranges from 32 bits to 448 bits, block ,block size is 64 bit, cipher. It considers 16 rounds of the feistel network along with S-boxes which depends on a key.

Step 4: Embedding of data using LSB Based Data Embedding Technique

Once the image is encrypted using the Blowfish algorithm in the previous step. Next steps involves in embedding the credential data to this encrypted image using LSB technique. In this process the least bit of the each byte of the image is replaced with the data. So as to ensure the proper length of embedded data any special or NULL character can be used as delimiter.



Step 5: Enter the Host Image for applying the RGB Based Steganography on Encrypted Embedded File

Any arbitrary host image is taken to stitch the RGB components of the image and the encrypted image. This is the image that will be seen to any intruder or the eavesdropper in the network which holds the encrypted image and the credential data in it.

Step 6: Resultant Image for Sending the Image to Receiver

After performing all the operations the image is ready to send to the receiver.

V. CONCLUSION

As the transmission over the network becomes easy and frequently used by the user it have cropped up with many of the unintended problems represented as attacks resulted into destroying the confidentiality, integrity and availability of the data present over the communication between two parties. We proposed a system through which we can dodge the attackers to an extent by successfully embedding the credential image and data as a single entity and making the attackers unknown of the data by encapsulating in a host image as the method so developed does not increase the size of the file to be transmitted significantly it can act as an extra layer of security and intruders and be avoided to an extent.

VI. FUTURE WORK

The system mainly deals with images that are suitable for maintaining the balance load in network and because of it we are limiting our size of embedded text along with the host images. If there is any abnormal increase in size of image the malpractices grows rapidly as intruders acknowledges to be fishy. So we can use lossless data compression algorithms to eradicate the amount of eavesdropping by intruders.

To use alpha-numeric value rather than the positive integers during the process of data embedding phase can also be considered as a future work for our project. We can also employ a technique such that more data can be embedded without much affecting the size of the file to be transmit.

Further using an encrypting algorithm that minimizes the CPU utilization will be more efficient.

REFERENCES

1. Dr. S.A.M Rizvi , Associate Professor,Department of Computer Science, JamiaMilliaIslamia, New Delhi,Dr. Syed Zeeshan Hussain, Assistant Professor, Deptt. of Computer Science, JamiaMilliaIslamia, New Delhi, "Performance Analysis of AES and TwoFish Encryption Schemes", 2011 *International Conference on Communication Systems and Network Technologies* ISSN:978-0-7695-4437-3/11.
2. B. Schneier, J. Kelsey, D. Whiting, D. Wagner,C. Hall, and N. Ferguson, "TwoFish: A 128-bit Block Cipher", AES submission, june 1998, http://www.counterpane.com/twofish.html.
3. Chun-Hsiang Huang, Shang-Chih Chuang, and Ja-Ling Wu, Fellow, "Digital-Invisible-Ink Data Hiding Based on SpreadSpectrum and Quantization Techniques", *IEEE TRANSACTIONS ON MULTIMEDIA*, VOL. 10, NO. 4, JUNE 2008.
4. Amritpal Singh, Dept. of Computer Science and Engineering, Harpal Singh University college of Computer Application Guru Kashi University Talwandi Sabo, India, "An improved LSB base Image Steganography Technique for RGB Images", 2015 *IEEE International Conference on Electrical, Computer and Communication Technologies* (ICECCT) ISSN 978-1-4799-6085-9/15.
5. Jyoti T.G. Kankonkar , Prof Nitesh Naik, Dept. of Compute Engineering, Goa College of Engineering,Farmagudi,Goa, India, "Image Security using Image Encryption and Image Stitching" , IEEE 2017 *International Conference on Computing Methodologies and Communication* (ICCMC)ISSN 978-1-5090-4890-8/17.
6. Neil Ferguson, "Impossible differentials in twofish", October 19**,** 1999.
7. Aparna. K, Jyothy Solomon, Harini . M, Indhumathi . V B.E (final year) Department of Computer Science and Engineering United Institute of Technology, Coimbatore, India,"A Study of Twofish Algorithm", 2016 *IJEDR* | Volume 4, Issue2 | ISSN: 2321-9939.
8. Sukhvandna Abhi,Umesh Sehgal,GNA University,Phagwara, IJCSN International Journal of Computer Science and Network,"A Review Analysis of Two Fish Algorithm Cryptography Quantum Computing", *IJCSN International Journal of Computer Science and Network*, Volume 6, Issue 1, February 2017.
9. Yong Zhang, Xueqian Li, Wengang Hou School of Software and Communication Engineering Jiangxi University of Finance and Economics Nanchang, P.R. China, "A Fast Image Encryption Scheme Based on AES", 2017 2nd *International Conference on Image, Vision and Computing* ISSN 978-1-5090-6238-6/17,.
10. Quist-Aphetsi Kester, MIEEE Lecturer, Faculty of Informatics Ghana Technology University College Accra, Ghana,"Image Encryption based on the RGB PIXEL Transposition and Shuffling", *I. J. Computer Network and Information Security*, 2013, 7, 43-50 Published Online June 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.07.05.
11. Jaspal Kaur Saini, Harsh K Verma, Department of Computer Science and Engineering National Institute of Technology Jalandhar, Punjab, India, "A Hybrid Approach for Image Security by Combining Encryption and Steganography",2013 IEEE Second (ICIIP-2013) ISSN 978-1-4673-6101-9/13,.
12. Dr.M.Umamaheswari,Prof.S.SivasubramanianS.PandiarajanDepartment of Computer Science and Engineering, Bharath University, Chennai-73, Tamil Nadu, India, " Analysis of Different Steganographic Algorithms for Secured Data Hiding", IJCSNS *International Journal of Computer Science and Network Security*, VOL.10 No.8,.
13. Purnima Gehlot,S. R Biradar,B. P. Singh, MITS University, Laxmangarh (Raj.), " Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL", *International Journal of Computer Applications* (0975 – 8887) Volume 70– No.13,.

14. Dr. S.A.M Rizvi , Dr. Syed Zeeshan Hussain, Neeta Wadhwa, Jamia Millia Islamia, New Delhi, *" Performance Analysis of AES and TwoFish Encryption Schemes", 2011 International Conference on Communication Systems and Network* Technologies ISSN 978-0-7695-4437-3/11,.
15. B. Lakshmi Sirishal, S. Srinivas Kumarl and B. Chandra Mohan, Bapatla Engmeenng College, Bapatla, Andhra Pradesh, India, "*Steganography based information security with high embedding capacity",*2015 *National Conference on Recent Advances in Electronics & Computer Engineering (RAECE).* G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
16. Tapan Kumar Hazra Department of Information Technology Institute of Engineering & Management, Salt Lake, Kolkata, Anisha Mahato Department of Information Technology Institute of Engineering & Management, Salt Lake, Kolkata, Arghyadeep Mandal Department of Information Technology Institute of Engineering & Management, Salt Lake, Kolkata, Ajoy Kumar Chakraborty Department of Information Technology Institute of Engineering & Management, Salt Lake, Kolkata, " A Hybrid Cryptosystem of Image and Text Files Using Blowfish and Diffie-Hellman Techniques".
17. Nilar Thein ,Hanung Adi Nugroho ,Teguh Bharata Adji,I Wayan Mustika department of Electrical Engineering and Information Technology, Faculty of Engineering, Universitas Gadjah Mada Jalan Grafika 2, Kampus UGM, Yogyakarta, Indonesia, " Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes" *2017 International Conference on Advanced Computing and Applications (ACOMP)* 978-1-5386-0607-0/17 $31.00 © 2017 IEEE DOI 10.1109/ACOMP.2017.25.
18. Madhumita Panda Lecturer ,Computer Science SUIIT, Sambalpur University Odisha, India, " Performance Analysis of Encryption Algorithms for Security" *International conference on Signal Processing, Communication, Power and Embedded System* (SCOPES)-2016, 978-1-5090-4620-1/16/$31.00 ©2016 IEEE.
19. Harpreet Kaur1, a and Jyoti Rani1 CSE Department, GZSCCET Bathinda, Punjab, India, " A Survey on different techniques of steganography", *MATEC Web of Conferences 57, 02003,* DOI 10.1051/matecconf/20165702003.
20. Manish chaudhary, Kamaldeep Joshi, Rajkumar Yadav, Rainu Nandal CSE Department, University Institute of Engineering and Technology, M. D. University, Rohtak, Haryana, India, ," Survey on Image Steganography and its Techniques", *International Journal of Engineering and Technology (IJET),* DOI: 10.21817/ijet/2017/v9i3/170903S049 Vol 9 No 3S July 2017.
21. Shreyank N Gowda, " Using Blowfish Encryption to Enhance Security Feature of an Image", *2016 6th International Conference on Information Communication and Management,* ,978-1-5090-3495-6/16/$31.00 ©2016 IEEE.
22. Mamta Jain, Pallavi Kumari Mody University Lakshmangarh, Rajasthan, India "A Survey on Digital Image Steganography using RGB Color Channel *" ,Suresh Gyan Vihar University International Journal of Environment, Science and Technology Volume 3, Issue 1, Jan 2017, pp.21-25*..

AUTHORS PROFILE

Deepanshu Agarwalis pursuing Bachelor of technology in Information technology at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune and a diploma holder in Network Security. He has been selected for the award of prestigious HSBC-BVUCOE Merit Scholarship. His research interests includeNetwork Security, Data Science and analysis, Artificial Intelligence.

Pravesh Panwar is pursuing Bachelor of technology in Information technology at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune and a diploma holder in Network Security. His field of interest includes artificial intelligence, data science and analysis along with network security.

Purva Vyas is pursuing Bachelor of technology in Information technology at Bharati Vidyapeeth (Deemed to be University) College of Engineering,Pune and a diploma holder in network security. Her field of interest includes artificial intelligence, data science and analysis along with research in network security.

Prof. T.B. Patilpursued Bachelor of Computer Engineering from Bharati Vidyapeeth College of Engineering, Mumbai University, India in year 2007 and Master of Computer Engineering from Bharati Vidyapeeth deemed to be University, Pune-43 India in year 2015. He is currently working as Assistant Professor in Department of Information Technology, Bharati Vidyapeeth Deemed to be University, Pune-43 India since 2010. He has published more than 16 research papers in reputed international journals including Scopus Journal and conferences which are available online. His main research work focuses on Computer Networks, Software Engineering, Computer Graphics and Image Processing. He has 8 years of teaching experience.

Prof. Dr. S. D JoshicompletedPhD in Computer Engineering from Bharati Vidyapeeth deemed to be University, Pune-43 India. He is currently working as Professor from last 27years in Department of Computer Engineering, Bharati Vidyapeeth Deemed to be University, Pune-43 India. He has published 215 research papers in reputed international journals including Scopus Journal and international conferences which are available online. His main research work focuses on Software Engineering.