IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE PHOTO SHARING USING HASH-MSB STEGANOGRAPHY WITH DWT AND RGB PIXEL SHUFFLING ENCRYPTION ALGORITHMS

R.Dhinakaran Samuel[1], J.Jose Maritta[2], G.Karthika[3], D.Ramyaa[4]
[1]Professor, Department of Computer Science and Engineering
[2,3,4]Final Year UG Students, Department of Computer Science and Engineering

DOI: 10.5281/zenodo.1252874

ABSTRACT

The proposed algorithm ensure the encryption and decryption using DWT and RGB pixel shuffling with steganography by using hash-most significant Bit (HMSB) that make use of hash function to be developed significant way to insert data bits in MSB bits of RGB pixels of cover image. The security evaluations are presented by calculating a peak signal to noise ratio and mean square error. Secret image, PSNR is infinity and MSE is 0. For cover image, PSNR is about 63 dB and MSE is about 0.03.The results show that high level of the similarity exists between the stego-images and cover images and the same is for secret images and extracted image as represented also in Histogram Analysis of secret images.We propose a novel method for key generation by using nearest prime pixels. Further 2's complement and logical operations are performed to generate decrypted image. The final decrypted image is generated by representing pixels in matrix form and data is retrieved in column wise.

KEYWORDS: Cryptography, DWT (Discrete Wavelet Transform), Hash-MSB, Decrypted Image, Encrypted Image, PSNR (Peak Signal to Noise Ratio), Pixel, Shuffling, and steganography.

I. INTRODUCTION

To improve information security through developing efficient image cryptography algorithm by using encryption with steganography. It looks random that means it can pass all the statistical tests of randomness we can find. It is unpredictable that is, even if complete knowledge of the algorithm, hardware, and all the previous bits are given, it is still computationally infeasible to predict what the next random bit will be. It cannot be reproduced reliably. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. Decryption is the process of taking encoded or encrypted text or other data and converting it back into textthat you or other computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Even if the generator runs twice with exactly the same input, two completely unrelated random sequences can be obtained. The encryption and decryption using DWT and RGB pixel shuffling with steganography by using hash-Most significant Bit (HMSB) that make use of hash function to developed significant way to insert data bits in MSB bits of RGB pixels of cover image

II. RELATED WORKS

A chaos-based colour image encryption scheme, the highlight is that the randomly sampled noise signal is applied to serve as the initial values of a chaotic system. The 256-bit hash value of noise is transformed into the one-time initial values of the Liu system. The sequences generated by Liu system are subjected to three batteries of TestU01. Exclusive OR, the only operation, is applied to diffuse the pixels, and some measures are taken to speed up the encryption process. Finally, some statistical tests are performed to assess reliability and efficiency of the proposed cryptosystem in terms of time complexity and security. Cipher algorithms are becoming more complex daily. Asymmetric key encryption algorithms the keys used for encryption and decryption must be different.

III. PROPOSED SYSTEM

Image encryption algorithms and hiding algorithms should be designed to enhance the effectiveness of transmission and keep safety from attacks by the intruders. The proposed method can achieve the highest level of data integrity, confidentiality and security. The meet in the middle attack attempts to find a value using both of the ciphertext and plaintext of the composition of block ciphers, such that the forward mapping through the first functions is the same as the backward mapping through the last functions, quite literally meeting in the middle of the composed function. The proposed encryption scheme is based on one-time keys and stream cipher, not block cipher, and only the XORoperation is employed, even if the attacker get some plaintext and ciphertext pairs, it is impossible to use these keys to decrypt the next cipher, because our scheme is based on onetime keys, they are unique and never be re-used.The symmetric key algorithm is used identically for encryption and decryption such that the data stream is simply XORed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Published procedures exist for cracking the security measures as implemented in WEP. The algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this encryption algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas. A modulo operation is the process of yielding a remainder from division. The main function of the pixel shuffling is that it involves no modification in the bit values and no expansion of pixels in the end of the encryption and the decryption procedure. The pixel values are redesigned and combined moving from their particular positions and then the values are swapped to give the cipher image which becomes recognizable.

IV. MODULES

a) Image pre-processing

Pre-processing is a common name for operations with images at the lowest level of abstraction - both input and output are intensity images. These iconic images are of the same kind as the original data captured by the sensor, with an intensity image usually represented by a matrix of image function values (brightnesses). The aim of pre-processing is an improvement of the image data that suppresses unwilling distortions or enhances some image features important for further processing, although geometric transformations of images (e.g. rotation, scaling and translation) are classified among pre-processing methods here since similar techniques are used. Image pre-processing methods are classified into four categories according to the size of the pixel neighbourhood that is used for the calculation of a new pixel brightness. Deals with pixel brightness transformations, Describes geometric transformations, Consider pre-processing methods that can used local neighbourhood of the processed pixel and briefly characterizes image restoration that requires knowledge about the entire image. Some classify image pre-processing methods differently into imageenhancement, covering pixel brightness transformations (local pre-processing in our sense), and image restoration. Image pre-processing methods use the considerable redundancy in images. Neighbouring pixels corresponding to one object in real images have essentially the same or similar brightness value, so if a distorted pixel can be picked out from the image, it can usually be restored as an average value of neighbouring pixels.

b) Cover Image and Secret Image

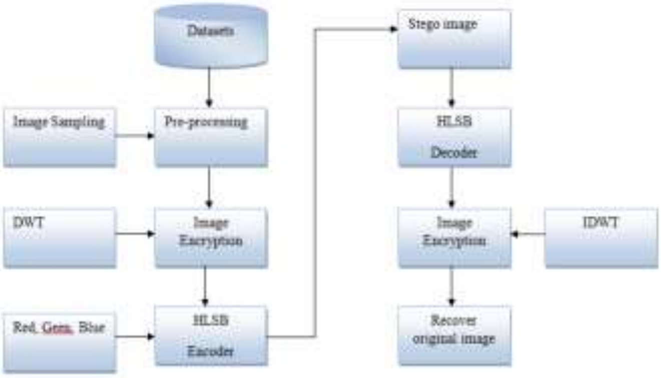
In our proposed system, first of all we select a true colour image of size 512 x 512 for to it as a cover image and a secret message which will be embedded in the cover image.

c) DWT(Discrete Wavelet Transform)

Steganography transmits data by hiding the existence of the message so that a viewer cannot identify the transmission of message and hence not able to decrypt it. This work proposes a data securing technique that is used for hiding multiple colo images into a single colour image using the Discrete Wavelet Transform.

d) MSB(Most Significant Bit)

Steganography has become one of the widely used tools in today's world for hiding information within another data or an image. It is a technique that takes cryptography to the next level by concealing the presence of a message itself. Data Encryption Standard algorithm is such a cryptographic key which is applied to a block of plain text to convert it into a cipher text and vice-versa. This paper presents an innovative idea to hide a message within an image of any dimension by encrypting the message through Data Encryption Standard algorithm and concealing the message by applying LSB encoding technique in a spiral manner thus enhancing the difficulty of the decoder. The main objective is that, securing of data becomes more potent and secretive than the previous ones.



Figure(1) Flow Diagram

Figure(1) shows the illustration for encryption and decryption process. And then figure(2) describes the algorithm, with a sample imagewith different illumination from Oulu face database , of preprocessing of the face images to obtain a segmented face from the input face image. From the obtained results we can conclude that the embedding capacity in the proposed algorithm is very good as shown in figure(3). The simulation of the above algorithm was performed using MATLAB. The experimental outcomes i.e. from figure(4) showed the proposed algorithm improves the embedding capacity, which maintains the quality of the stego-image, more efficient, simple, appropriate and accurate than other algorithms, as well as it makes the secret image more secure.

V. RESULT ANALYSIS

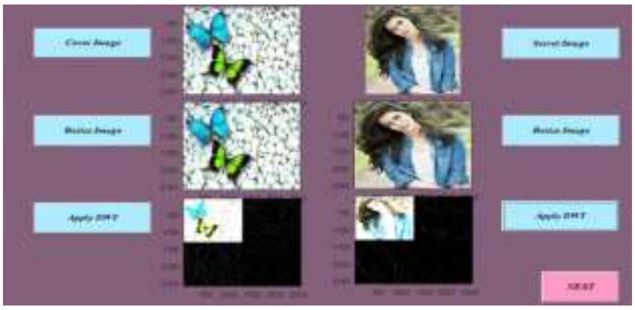
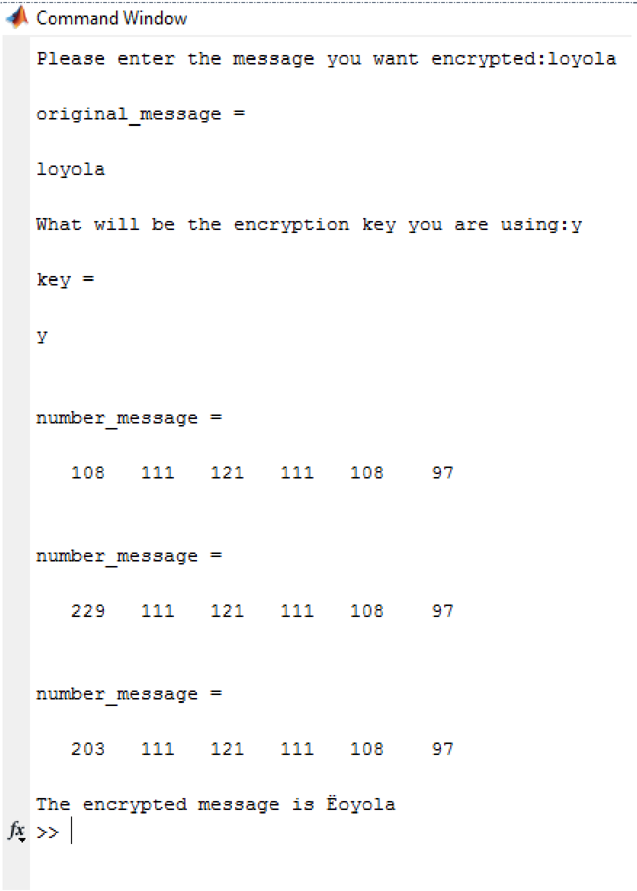
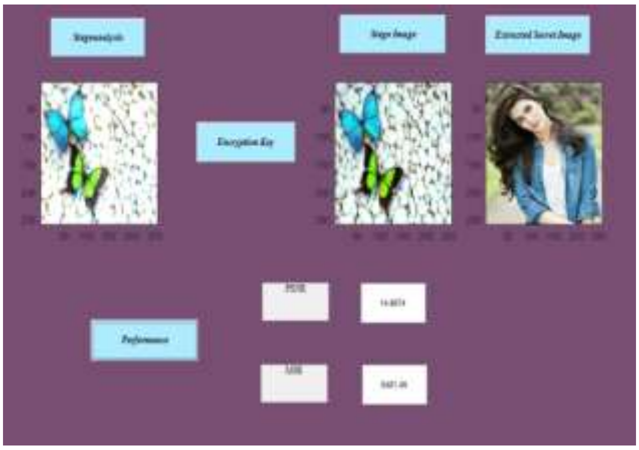


Figure (2) Encrypted Image



```
Please enter the message you want encrypted:loyola

original_message =

loyola

What will be the encryption key you are using:y

key =

y


number_message =

   108   111   121   111   108    97


number_message =

   229   111   121   111   108    97


number_message =

   203   111   121   111   108    97

The encrypted message is Ëoyola
>> |
```

Figure(3) Encryption Key



Figure(4) Decrypted Image

VI. CONCLUSION

The Cryptography techniques DWT & RGB Shuffling algorithm has been implemented to encrypt the secret image(jpg, png, gif, and bmp) before embedding it in the RGB cover image(jpg, png, gif, and bmp) with the goal that it is difficult to intruder to detect the encryption. Image encryption using DWT and Shuffling encryption has a considerable security quality factor which implies the intensity distributions for the original images and mutilated image are distinctive. Three state variable sequences of Liu system are applied to diffuse the red, green and blue components through bitwise XOR operation. The running speed is effectively improved by some time-saving operations, such as effectively determine iterative times according to image size, faster integer operations, exactly amplification factor of state variables, matrix calculation and pre-allocated memory.

The experimental results have demonstrated the effectiveness of the fast colour image encryption scheme. To evaluate this system we tested a number of images to be encrypted and hidden with the proposed algorithms.

VII. FUTURE ENHANCEMENT

According to the tested we found that the system has provide a high security and easy way to encrypt, embedding and decrypt secret image without effecting the quality of images(secret or cover) as appeared in measurements of (MSE , PSNR and security quality).

VIII. REFERENCES

[1] Cheddad, J. Condell, K. Curran, and P. MC Kevitt, "A Secure and improved Self-embedding algorithm to Combat Digital Document Forgery," *signal processing*, vol. 89, pp. 2324-2332, 2009.

[2] X.-Y. Wang, C.-P.Wang, H.-Y.Yang, and P.-P. niu, "A Robust blind colour image watermarking in quaternion Fourier Transform Domain," *journal of systems and software*, vol. 86, pp. 255-277, 2013.

[3] M. Sajjad, ET AL., "Mobile-cloud assisted framework for selective encryption of medical images with steganography for Resource-Constrained Devices," *multimedia tools and applications*,vol. 76, pp. 3519-3536, 2017.

[4] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: a survey," *computer science review*,vol. 13–14, pp. 95-113, 2014.

[5] S. Islam, M. R. Modi, and P. Gupta, "Edge-based image steganography," *eurasip journal on information security*,vol. 2014, pp. 1-14, 2014.

[6] M. Hasnaoui and M. Mitrea, "Multi-symbol qim video watermarking," *signal processing: image communication*,vol. 29, pp. 107-127, 2014.

[7] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the klt tracking algorithm and bch codes," *in 2015 IEEE long island systems, applications and technology conference (lisat)*, 2015, pp. 1-7.

[8] K. Qazanfari and R. Safabakhsh, "A new steganography method which preserves histogram: generalization of lsb++," *information sciences*,vol. 277, pp. 90-101, 2014.

[9] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "Adaptive steganography based on syndrome-trellis codes and local complexity," *in 2012 fourth international conference on multimedia information networking and security (mines)*, 2012, pp. 323-327.

[10] A. Singh, B. Kumar, S. Singh, S. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using back propagation neural network," *future generation computer systems*, 2016.

CITE AN ARTICLE

Samuel, R., Maritta, J., Karthika, G., & Ramyaa, D. (2018). SECURE PHOTO SHARING USING HASH-MSB STEGANOGRAPHY WITH DWT AND RGB PIXEL SHUFFLING ENCRYPTION ALGORITHMS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(5), 490-495.

.