Encrypting and Decrypting an RGB Image

Rajendra Prasad Sahu, Avinash Sharma

Abstract - The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc. Image encryption and decryption are essential for securing images from various types of security attacks. Earlier proposed schemes for encryption and decryption of images on each and every layer (red, green, blue) so its taking the maximum time. Our proposed approach, keys and the arrangement of RMAC parameters are mandatory. If we use the color index image instead of "RGB", we have to encrypt only one layer (map) which reduced the 1/3 encrypted time approximately. We have also formulated a formula for all the possible range to choose keys for encrypting and decrypting an RGB image. So this approach can be used for transmission of RGB image data efficiently and securely through unsecured channels.

Keyword: PNG Image, SVD HASH and AES, USART, PWM, Microcontroller.

I. INTRODUCTION

Encryption is a common technique to uphold multimedia image security in storage and transmission over the network. It has application in various fields including internet communication, medical imaging and military communication. Due to some inherent features of images like high data redundancy and bulk data capacity, the encryption of image differs from that of text, thus algorithms suitable textual data may not be suitable for multimedia data.

Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys.

Enormous number of transfer of data and information takes place through internet, which is considered to be most efficient though it's definitely a public access medium.

The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc. One of the best-known techniques of visual cryptography has been credited to Moni Naor and Adi Shamir. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

The chaotic confusion and pixel diffusion methods were proposed by Friedrich perform the permutations using a chaotic 2-D combined with alterations of Grey-Level values of each pixel in a sequential manner. Repetitive rounds of permutations and changes were used to achieve higher security. It was experimentally verified that the amount of time overhead in performing complex calculations and the complex diffusion process had led to large time complexity of the system.

When Visual Cryptography is used for secure communications; the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

The main objective of this concept is to develop high security for transmission of images in an open network. Here, the encryption approach is based on Two Stage Random Matrix Affine Cipher (TSRMAC) associated with Discrete Wavelet Transformation (DWT) is designed to ensure secure transmission of image data. Security of images has become an important agenda of the present era. Network and communication technologies provide several modes for transfer-ring images all over the world. Images are frequently used in diverse areas such as defense services, engineering services, scientific experiments, medical imaging, advertising, art exhibition, online education and training.

With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting images for confidentiality, integrity, authentication, and non-repudiation is a major concern. Several methods have been proposed to encrypt and decrypt image data securely.

1. Two Stage Random Matrix Affine Cipher and Discrete Wavelet Transformation

Here taking RMAC on an RGB image of size n m. The pixels of an RGB image is given in matrix form in which even numbered rows and columns are shifted by parameters α and γ, and multiplied by parameters χ and λ, respectively. Odd numbered rows and columns are shifted by parameters β and δ, and multiplied by parameters η and s, respectively. Multiplier parameters χ and η are relatively prime to m, whereas multiplier parameters λ and s are relatively prime to n, $0o\alpha \neq \beta om$ and $0o\gamma \neq \delta on$.

Owing to the advance in network technology, information security is an increasingly important problem. Popular application of multimedia technology and increasingly transmission ability of network gradually lead us to acquire information directly and clearly through images. Hence, image security has become a critical and imperative issue. Image encryption techniques try to convert an image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-tv, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed, but some of them have been known to be insecure, so we always in need to develop more and more secure image encryption techniques. Traditional data encryption techniques can be divided into two categories which are used individually or in combination in every cryptographic algorithm: substitution and transposition. In substitution technique, we symmetrically replace one symbol in the data with another symbol according to some algorithm; in a transposition technique, we reorder the position of symbols in the data according to some rule.

Many image-protection techniques use vector quantization (VQ) as the main encryption technique. A symmetric block encryption algorithm creates a chaotic map, used for permuting and diffusing multimedia image data. There have been many more image encryption algorithms based on chaotic maps. Also other encryption algorithms based on concepts such as block cipher and selective encryption has been proposed. A few techniques focus on video encryption. Several cryptosystems similar to data encryption, such as steganography and digital signature have also been implemented to increase security of multimedia data storage and transmission. The approach uses concept of uniform scrambling, row, column and block based image shuffling to reduce correlation. Further, encryption is performed using a chaotic sequence generated by symmetric keys to ensure the security of the proposed algorithm.

In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. The reverse process is referred to as decryption. Cryptography has evolved from the from classical such as Caesar, Vigenère, Trifid ciphers to modern day cipher and public key systems such as Diffie-Hellman etc[2] Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys.

The encryption and decryption process of this paper is based on symmetrical algorithm encryption process. Typical examples symmetric algorithms are Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent.

II. RELATED WORK

In 2013 by Manish Kumara et. Al. Proposed a approach, keys and the arrangement of RMAC parameters are mandatory and also formulated a formula for all the possible range to choose keys for encrypting and decrypting an RGB image. Computer simulation with a standard example and result is given to analyze the capability of the proposed approach and given security analysis and comparison between our proposed technique and others to support for robustness of the approach. This approach can be used for transmission of image data efficiently and securely [1].

By the Quist-Aphetsi Kester gives the concept about encryption methods for enhancing the security of digital contents has gained high significance in the current area of breach of security and misuse of the confidential information intercepted and misused by the unauthorized parties. Rigorous use of advanced mathematical algorithms has played a major role in the success of modern day cryptography and contribute to the general body of knowledge in the area of cryptography application and by developing a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel.

In 2012 by Ali A.Yassin aims to create two encryption algorithms and which have the ability to partial encryption of any image by using the key to be chosen from another image, both algorithms depend on techniques to analyze the image into three layers (RGB / YIQ) for both images entered and tagged. The next step is to determine the specific number for both images to select bit from each pixel of one of the three layers for both image tagged or the input image and then apply the XOR operation between the two bits opposing both classes of the input image and the image of the key. As a result of the last operation leads to encrypt three layers, both based on the RGB or YIQ and then they are incorporated into class's encoded leads to obtain the encrypted part. The strength of both algorithms how to find one key first and then specify the layer as second and then know the number of bit action chosen Third, where will be generated to have a space key is very much depends on image size, leading to difficult to break, but scales standards that are the similarities and the likelihood that the balance algorithm YIQ to RGB as well as processing speed and focused on the part of the image instead of dealing with all the data in addition to the difficulty in projecting the key through the very large key space.

The encryption methods for enhancing the security of digital contents has gained high significance in the current era of breach of security and misuse of the confidential information intercepted and misused by the unauthorized parties. This paper sets out to contribute to the general body of knowledge in the area of cryptography application and by developing a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel.

Here author introduce a novel scheme for separable reversible data hiding in encrypted domain in which we use image as a cover medium. This paper illustrates the various objectives of implementing separable reversible data hiding technique. The separable reversible data hiding is consists of three steps in the first step; a content owner encrypts the image using an encryption key. Then, a data-hider compresses the encrypted image using a data-hiding key. The third step is to extract the additional data and recover the original image. The activities i.e. extracting the additional data and recover the original images are depends upon which key the receiver has. There is separation of these two activities according to availability of keys. The scheme's main feature is the way of data embedding into the encrypted image using the different positions of LSB within image. Here we are concentrating on using RGB-LSB method for data embedding and finally verifies the performance of using RGB-LSB method in terms of data capacity, image quality etc.

The method proposed in this paper, breaks this correlation increasing entropy of the position and entropy of pixel values using block shuffling and encryption by chaotic sequence respectively. The plain-image is initially row wise shuffled and first level of encryption is performed using addition modulo operation. The image is divided into blocks and then block based shuffling is performed using Arnold Cat transformation, further the blocks are uniformly scrambled across the image. Finally the shuffled image undergoes second level of encryption by bitwise XOR operation, and then the image as a whole is shuffled column wise to produce the ciphered image for transmission. The experimental results show that the proposed algorithm can successfully encrypt or decrypt the image with the secret keys, and the analysis of the algorithm also demonstrates that the encrypted image has good information entropy and low correlation coefficients.

This paper presents a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. The novelty of this work lies in deploying the concept of keyed discrete Fourier transform (DFT) followed by DE operations for encryption purpose. To this end, a secret key is shared between both encryption and decryption sides. Firstly two dimensional (2-D) keyed discrete Fourier transform is carried out on the original image to be encrypted. Secondly crossover is performed between two components of the encrypted image, which are selected based on Linear Feedback Shift Register (LFSR) index generator. Similarly, keyed mutation is performed on the real parts of a certain components selected based on LFSR index generator. The LFSR index generator initializes it seed with the shared

secret key to ensure the security of the resulting indices. The process shuffles the positions of image pixels. A new image encryption scheme based on the DE approach is developed which is composed with a simple diffusion mechanism. The deciphering process is an invertible process using the same key. The resulting encrypted image is found to be fully distorted, resulting in increasing the robustness of the proposed work. The simulation results validate the proposed image encryption scheme.

By the author present and study a newly designed digital image scrambler (as part of the two fundamental techniques used to encrypt a block of pixels, i.e., the permutation stage) that uses knight's moving rules (i.e., from the game of chess), in conjunction of a chaos-based PRBG, in order to transpose original image's pixels between RGB channels. Theoretical and practical arguments, rounded by good numerical results on scrambler's performances analysis (i.e., under various investigation methods, including visual inspection, adjacent pixels' correlation coefficients' computation, key's space and sensitivity assessment etc.) confirm viability of the proposed method (i.e., it ensures the coveted confusion factor) recommending its usage within cryptographic applications.

A new cryptographic scheme proposed for securing color image based on visual cryptography scheme was done by Krishnan, G.S. and Loganathan, D. A binary image was used as the key input to encrypt and decrypt a color image. The secret color image which needs to be communicated was decomposed into three monochromatic images based on YCbCr color space. Then these monochromatic images were then converted into binary image, and finally the obtained binary images were encrypted using binary key image, called share-1, to obtain the binary cipher images. During their encryption process, exclusive OR operation was used between binary key image and three half-tones of secret color image separately. These binary images were combined to obtain share-2. In the decryption process, the shares were decrypted, and then the recovered binary images were inversed half toned and combined to get secret color image. [9]

With extended Visual Cryptography, which is a method of cryptography that reveals the target image by stacking meaningful images. Christy and Seenivasagam proposed a method that uses Back Propagation Network (BPN) for extended visual cryptography. BPN was used to produce the two shares. The size of the image produced was the same as that of the original image. [10]

A k-out-of-n Extended Visual Cryptography Scheme (EVCS) is a secret sharing scheme which hides a secret image into n shares, which are also some images. The secret image can be recovered if at least k of the shares are superimposed, while nothing can be obtained if less than k shares are known. Previous EVCS schemes are either for black-and-white images or having pixel expansion. Wu, Xiaoyu, Wong, Duncan S. and Li, Qin proposed the first k-out-of-n EVCS for color images with no pixel expansion. The scheme also improved the contrast of the n shares and the reconstructed secret image (i.e. the superimposed image of any k or more shares) by allowing users to specify the level of each primary color (i.e. Red, Green and Blue) in the image shares as well as the reconstructed secret image. [11]

Kester, QA proposed a cryptographic algorithm based on matrix and a shared secrete key.[11]. Which was further applied encryption and decryption of the images based on the RGB pixel [12].

Shujiang Xu,Yinglong Wang , Yucui Guo and Cong Wanga proposed a novel image encryption scheme based on a nonlinear chaotic map (NCM) and only by means of XOR operation. There were two rounds in the proposed image encryption scheme. In each round of the scheme, the pixel gray values were modified from the first pixel to the last pixel firstly, and then the modified image was encrypted from the last pixel to the first pixel in the inverse order. In order to accelerate the encryption speed, every time NCM wasiterated, n (n>3) bytes random numbers were used to mask the plain-image. And to enhance the security, a small perturbation was given to the parameters of the NCM based on the last obtained n bytes modified elements before next iteration. [13].

Control parameters were utilized to generate chaotic orbits applied to scramble the pixel positions while one coupled map lattice was employed to yield random gray value sequences to change the gray values so as to enhance the security. Experimental results have been carried out with detailed analysis to demonstrate that the proposed image encryption scheme possesses large key space to resist brute-force attack and possesses good statistical properties to frustrate statistical analysis attacks. And at the end, the proposed scheme utilizes the 3D skew tent map to shuffle the plain-image efficiently in the pixel Positions permutation process and it employed the coupled map lattice system to change the gray values of the whole image pixels greatly [14].

With the exceptionally good properties in chaotic systems, such as sensitivity to initial conditions and control parameters, pseudo-randomness and ergodicity, chaos-based image encryption algorithms have been widely studied and developed in recent years. Standard map is chaotic and it can be employed to shuffle the positions of image pixels to get a totally visual difference from the original images. Ruisong Ye,Huiqing Huang proposed two novel schemes to shuffle digital images. Different from the conventional schemes based on Standard map, they disordered the pixel positions according to the orbits of the Standard map. The proposed shuffling schemes didn't need to discretize the Standard map and own more cipher leys compared with the conventional shuffling scheme based on the discretized Standard map. The shuffling schemes were applied to encrypt image and disarray the host image in watermarking scheme to enhance the robustness against attacks. [15]

Amnesh Goel and Nidhi proposed contrastive methods to encrypt images by introducing a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption. [16]

Image Encryption Based on Explosive Inter Pixel Displacement of the RGB Attribute of a Pixel: In this method focus was more on the inter pixel displacement rather than just manipulation of pixel bits value and shifting of pixel completely from its position to new position. RGB value of pixel was untouched in this method, but R value of pixel jumps to another location horizontally and vertically same as in chaotic method. In the similar manner, G and B values of pixel [17].

III. PROBLAM STATEMENT

Image encryption and decryption are essential for securing images from various types of security attacks. Earlier proposed schemes for encryption and decryption of images on each and every layer (red, green, blue) so its taking the maximum time.

IV. PROPOSED WORK

Our proposed approach, keys and the arrangement of RMAC parameters are mandatory. If we use the color index image instead of "RGB",we have to encrypt only one layer(map) which reduced the 1/3 encrypted time approximately. We have also formulated a formula for all the possible range to choose keys for encrypting and decrypting an RGB image. So this approach can be used for transmission of RGB image data efficiently and securely through unsecured channels.

V. CONCLUSION

With the help of color index image we can reduce the time complexity of RGB and also provide the security on one level. So this approach can be used for transmission of RGB image data efficiently and securely through unsecured channels.

REFFERENCES

[1]. Manish Kumara,n, D.C. Mishrab, R.K. Sharmab," A first approach on an RGB image encryption" Optics and Lasers in Engineering 52 (2014) 27–34 Elsevier-2013.

[2]. Quist-Aphetsi Kester, MIEEE "A cryptographic Image Encryption technique based on the RGB PIXEL shuffling" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)ISSN: 2278 – 1323,Volume 2, Issue 2, January 2013

[3]. Ali A.Yassin "Design New Algorithm For Partial Image Encryption Based colors Space "Journal of Babylon University/Pure and Applied Sciences/ No.(2)/ Vol.(20): 2012

[4]. Quist-Aphetsi Kester, "Image Encryption based on the RGB PIXEL Transposition and Shuffling" I. J. Computer Network and Information Security, 2013, 7, 43-50 Published Online ,in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.07.05. June 2013

[5]. Vinit K Agham , Tareek M Pattewar "separable reversible data hiding technique based on rgb-lsb method", International Journal of Research in Advent Technology (IJRAT) Vol. 1, No. 3, , ISSN: 2321–9637, October 2013

[6]. Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B "Multilevel Image Encryption "Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal,2011.

[7]. Ibrahim S I Abuhaiba1 And Maaly A S Hassan "Image Encryption Using Differential Evolution Approach In Frequency Domain "Signal & Image Processing : An International Journal(Sipij) Vol.2, No.1, March 2011.

[8]. Adrian-Viorel DIACONU1 and Alexandru COSTEA "Color Image Scrambling Technique based on Transposition of Pixels between RGB Channels using Knight's Moving Rules and Digital Chaotic Map ",2011.

[9]. Krishnan, G.S.; Loganathan, D.; , "Color image cryptography scheme based on visual cryptography," Signal Processing, Communication, Computing and Networking Technologies

(ICSCCN), 2011 International Conference on , vol., no., pp.404-407, 21-22 July 2011.

[10]. Christy, J.I.; Seenivasagam, V.; , "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images," Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on , vol., no., pp.1101-1108, 21-22 March 2012.

[11]. Wu, Xiaoyu; Wong, Duncan S.; Li, Qing; , "Extended Visual Cryptography Scheme for color images with no pixel expansion," Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on , vol., no., pp.1-4, 26-28 ,July 2010

[12]. Kester, Quist-Aphetsi; Koumadi, Koudjo M;"Cryptographie technique for image encryption based on the RGB pixel displacement," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.74-77, 25-27 Oct. 2012

[13]. Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68, 2010.

[14]. Ruisong Ye,Wei Zhou,"A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", IJCNIS, vol.4, no.1, pp.38-44, 2012.

[15]. Ruisong Ye,Huiqing Huang, "Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking", IJIGSP, vol.2, no.1, pp.19-29, 2010.

[16] Amnesh Goel,Nidhi Chandra,"A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement", IJIGSP, vol.4, no.2, pp.16-22, 2012.

[17] Reji Mathews, Amnesh Goel, PrachurSaxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, San Francisco, USA. ISBN: 978-988-18210-9-6. 2011.

AUTHOR'S PROFILE

Rajendra Prasad Sahu pursuing master of technology in computer science, oriental collage of technology, Rajiv Gandhi proudyogiki vishwavidyalaya Bhopal. Madya Pradesh, India, PH-8871084147.

Avinash Sharma, Oriental Collage of Technology, Rajiv Gandhi proudyogiki vishwavidyalaya Bhopal. Madya Pradesh, India, PH-7415249228.