e-ISSN 2320 –7876 www.ijfans.org
Vol.11,S Iss 1, 2022
 UGC CARE Listed (Group -I) Journal

Encryption and Decryption using Steganography and Cryptography for Medical data Security-A Review

[1]Mayank Verma, [2]Dr.Ajay Kushwaha

[1]Research Scholar, [2]Professor,

[1-2]Deptt. of Computer Science, Rungta College of Engineering and Technology, Bhilai, CG, India

ABSTRACT- A cryptographic technique for protecting medical data picture is proposed based on visual cryptography. A protected picture and a binary image as a key to encrypt and decode are used as input. The YCbCr color scheme is used to divide a secret color image into three monochrome images that must be communicated. The monochromatic photographs are then converted into binary images, which are subsequently encrypted with a binary key image known as share-l to generate binary cypher images. The Exclusive OR operation is used to encrypt the binary key image and the three half-tones of the secret color picture. By mixing these binary images, Share-2 is formed. By mixing these binary images, Share-2 is formed. The parts are decrypted, and the recoverable binary pictures are halftoned and blended to create the secret shade image. This method is more successful for transmitting natural sights through unsecure channels.

Keywords-color image encryption; Medical; x-ray ; half-tone; inverse half-tone

I. INTRODUCTION

"A picture is worth a thousand words," as the saying goes, since it may provide more pictorial information than information acquired from a text for human interpretation. As a result, picture data representation, storage, and transmission must be acceptable. Information security is becoming increasingly important in data storage and transit. Images are employed in a variety of operations since they may contain significantly more info. Because digital images are utilized in a variety of industries such as medicine, the military, and private businesses, the safety of these contents is critical, which is why visual cryptography and decryption methods play a significant role in image data protection. Cryptography is a method of providing safe communication between two gatherings in a public place inhabited by unapproved clients and malicious attackers Encryption and decoding are two cryptography techniques that occur at the transmitter and collector closes, respectively. Encryption is the process of combining essential mixed media. files data with some extra data to transform it into an unread encoded format known as "Cipher" (known as key). Decryption is the inverse of encryption in that it uses the same or a different supplementary data (key) to decode the cypher and transform it to the

real multimedia data [9]. Another word is cryptanalysis, which refers to the techniques that an intruder can employ to study and breakdown down the encrypted statement between two parties [10]. Cryptography approaches can be classified according on their fundamental concepts or protocols. However, in this survey, we will focus on two types of cryptographic techniques: classical cryptography and quantum cryptography. Classical cryptography is mathematical in nature and is predicated on the computational complexity of factoring huge numbers. The security of traditional cryptosystems is predicated on the tremendous hardness of the mathematical problem for big number factorization. Furthermore, classical cryptosystems are classified into two types: Asymmetric and Symmetric Systems Quantum cryptography, on the other hand, is based on science and depends on quantum mechanics rules. It is a new technology that emphasises quantum physics phenomena, allowing two people to communicate securely based on the invariabilities of quantum theory principles. Quantum physics is the numerical approach or collection of ideas that enables the construction of physical theories. Two critical features of quantum physics on which quantum cryptography is based: Photon Polarization Principle and Heisenberg Uncertainty Principle.

II. RELATED WORK

The graphic cryptography changed into to start with presented and used most effective on binary images. Recently, some visual cryptography schemes for grey and coloration photo have been proposed.

In 1996, Naor and Shamir [2] presented VCS (okay,n), the thought of a cowl-based semi-bunch, to additionally work on the appraisal. Ateniese et al. [3] made the primary VCS (2,n) with the most ideal differentiation for each nl2. In 1997, Verheul and Tilborg [4] are quick to lay out a mystery imparting component for photos to c tones. The essential thought behind this framework is to partition one picture pixel into b subpixels, with each subpixel isolated into c variety regions. Each sub-pixel has precisely one hued conceal region, while any remaining shade areas are dark. The shade of one not entirely set in stone by the communications of the stacked sub-pixels. The nature of the found secret still up in the air by the regular range of shades and subpixels, which is a critical impediment of this procedure. Whenever the variety bed is enormous, shading the sub-pixels turns into a significant trouble. Tzung-Her Chen et al [5] anticipated a multi-mystery and approaches cryptographic methods that goes past customary apparent secret sharing. The codebook of conventional visual spine chiller sharing utilized to create extent depictions full scale block via full scale block all together that a couple of secret photos are presently just extent photographs and translate every one of the secrets individually by stacking two of percent photographs in a way of moving.

This technique might be used for various double, grayscale, and conceal secret pictures with pixel development. In [9], a cross breed arrangement using Watermarking and Cryptography was portrayed for the conveyance of a covered text based content message. This framework is basically founded on the XOR figure, the

Fibonacci assortment, the PN assortment, RSA, the Hill figure, the slightest bit, no-account, and three piece Least Significant Bit (LSB). They utilized the ideas of Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Mean Square Error (MSE) to assess the exceptionality of watermarked photographs (MSE). It was found that the slightest bit LSB watermarking continued to 2-cycle LSB watermarking and 3-digit LSB watermarking since MSE and RMSE were low and PSNR was high. They gave variable-period input messages that were scrambled and decoded utilizing cryptography methods, and the encoded message was masked utilizing three unmistakable LSB watermarking procedures. Jai Singh, Kamil Hasan, and Ravinder Kumar [10] explored cross breed cryptographic encryption approaches as well as the utilization of a few encryption philosophies to work on their level of safety and security to examine their mixture of crossover strategies, which enveloped the blend of cryptographic and virtual watermarking techniques. As far as security, the half and half technique was demonstrated to be more helpless against programmers and unlawful unscrambling of information was troublesome. Pooja Rani and Apoorva Arora contributed the utilization of Steganography for Image Security System. For a couple of photograph security structures. A large portion of the common photo insurance structures aren't date's place to watch contrary to the least digital assaults.

In [11] MATLAB became utilized for The framework's execution and design To decrease the size of the steganographic photo, pressure was applied. The undeniable realities (picture) may be disguised behind a selective photo. The genuine and face picture insights are checked in the group based steganographic technique, and any place the variety plans of the genuine and face picture are comparative, the real picture can be embedded in those pieces of the face picture [11]. Due to the reassuring outcomes acquired from their utilization in the domain of cryptography, the top pressure calculations investigated here are Discrete Cosine Conversion (DCT), Discrete Fourier Transform (DFT), and Wavelet Transform Transformation (DWT) (grouping). The period of time spent inside the framework can be determined. PSNR and MSE have additionally been determined for explicit boundaries to evaluate photograph quality.

III. CRYPTOGRAPHY

Cryptography is said to have grown with the skill of writing. As civilizations advanced, humans became ordered into tribes, clans, and kingdoms. As a result, notions such as power, battles, domination, and politics appeared. These ideas fueled people's natural desire to communicate anonymously with select recipients, assuring the further advancement of encryption. The beginnings of cryptography may be traced back to the Roman and Egyptian civilizations. Plaintext refers to information that must be kept secret. It is the original text, which might be characters, numbers, executable programmers, photographs, or any other sort of data. For example, plaintext is the text reaching the receiver after decryption or the transfer of a message in the sender's name earlier encryption.

Types of Cipher

1) Hill Cipher Method

2) Homophonic Substitution Cipher

3) Monoalphabetic Cipher

4) Ceaser Cipher

A. Hill Cipher Method

The Hill cipher is a polygraphed substitution linear algebra-based cypher Lester S. Hill invented it in 1929, and it became the first polygraphed cypher that was feasible (albeit barely) to perform on more than three symbols at the time.

1) Encryption: A modulo 26 integers is used to represent each letter. Though it is no longer a critical feature of encryption, this straightforward technique is nevertheless widely used: An invertible n framework is used to enhance each square of n characters to scramble a message (called a n-part vector). To decrypt the message, each square is replicated by the encryption grid's inverse. The encryption lattice is the coding secret, and it should be chosen at random from the arrangement of invertible n grids (modulo 26). Obviously, the code may be modified to any letters in any sequence with many letters; the arithmetic only has to be performed modulo the number of characters. With tendency to modulo 26. 2) Deciphering: To decode the message, we convert the cypher text into a vector and multiply this with the aid of the inverse matrices of the matrix (IFKVIVVMI in letters).

B. Homophonic Substitution Cipher

Because of Homophonic Substitution, Frequency Distribution became a less effective cryptanalysis tool. The fundamental rule of agreeably substitution is to assign a letter or image to the high frequency letters. You could, for example, use six different graphics to address "e" and "t," two signs to address "m," and one sign to address "z." Clearly, this encryption will need a larger jargon than letters, as each letter prefers at least one code text letter, and many like more. The most common method is to incorporate numerals inside the cypher text language, but you may also use a mix of capital, lower, and wrong way up letters. Some people even construct their own customized symbols to use. To preserve the characters of the cipher - text alphabet, we will employ a key of some form, similar to the Mixed Alphabet Cipher. Similarly, we employ the letters from the keyword first, with no repetitions, followed by the relaxation of the alphabet. We use significantly more letter clumping in the homophonic example, as well as more symbols to represent the 26 letters. The letter frequencies following a Cipher with Mixed Alphabets A nomenclator is a type of homophonic substitution cypher. This is a combination of a codebook and a huge homophonic substitution cypher. It was called after the persons who notified the presence of dignitaries and began with a little codebook containing the names of celebrities. This, however, quickly grew to include numerous common terms, phrases, and locations. The code and cypher components are not visible when written. Nomenclators had been a very effective cypher, and many of them had stayed unbroken for many years. In reality, there are a few pieces in achieves that have not been broken and provide fascinating insights into past stories.

C. Monoalphabetic Cipher

Because Caesar cypher and a adapted version of Caesar cypher are easily broken, monoalphabetic cypher enters the picture. In monoalphabetic literature, any alphabet may be substituted with the help of any other alphabet save the original alphabet. That is, every other letter from B to Z may be used to replace A. B can be substituted by A, C, or Z. C may be transformed to z by going through A, B, and D, and so on. Because there are multiple substitutions and a great range of permutation and combination, it is difficult to decipher the message using a mono alphabetic cypher. A monoalphabetic encryption is one in which each picture in plain text is assigned a hard and fast value. The relationship between a person in the visible text and a human inside the encrypted message is one-to-one. Each alphanumeric char of plain text corresponds to a special alphabetic character of encrypted textual material. If the key cost does not depend on the location of the seen text - based man or woman in the seen text - based flow into, the circulation cypher is monoalphabetic. It is a straightforward encryption method that is easy to understand and execute. We have a total of 26 possible keys. As a result, the brute-force assault observed artwork right here. A Confuse the two Cipher is an encryption method that employs the same static mapping from valid text to cipher letters throughout the text.

D. Ceaser Cipher

It is a replacement cypher, which means that every letter of the alphabet is substituted with a letter located a particular no. of places down the alphabet. A ceaser encryption is also known as a ceaser's cipher, the shift cypher, ceaser's code, or ceaser shift in cryptography. It is one of the simplest and most extensively used encryption methods. The amount of od letters used it to move the cypher alphabets defines Caesar cyphers.

Encryption Alternatively, the encryption algo may be stated using arithmetic by first converting the letters into integers, as in A 0, B 1..., Z 25. Encryption of a letter x by a shift n may be expressed mathematically as,

Mod 26 * Encryption(x)=(x+n)

Decryption Caesar's code

Decryption change one letter with another an reverse alphabet: a previous message in the alphabet.

IV. PROPOSED WORK

The Homomorphic algorithm is used for encryption and decryption in this case. We use watermarking on the picture for security reasons. PyCharm programmed is being used for results and simulation. Figure 1 depicts the entire procedure.

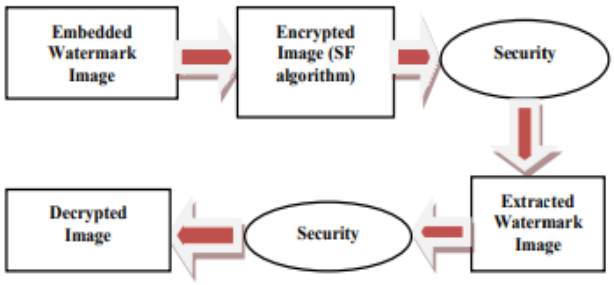

Fig.1: Process of the cryptography

Algorithm for hybrid digital watermarking and cryptography: -

Step 1: Open an image.

Step 2: Insert a text into the original picture file.

Step 3: We blur the image using the embedded approach.

Step 4: Change the original image to grayscale.

Step 5- Input a certain key utilizing the key expansion and selection method.

Step 6: Encrypt the blur picture with the SF technique to obtain an encrypted image that may be noisy.

Step 7: Apply the created passkey to the image cypher.

Step 8: Using the removal approach, obtain the grayscale image.

Step 9: Configure the integrated level security system open and decrypt an image using a password and an OTP.

The above method was tested on a standard picture.

Figures 2 and 3 provide a brief overview of the new encryption and decryption/recovery mechanisms. The figures represents the key created by the aforementioned procedure.

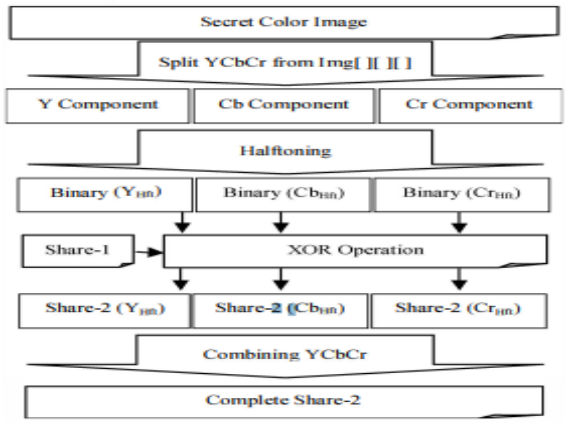

Fig. 2. Flow of encryption technique

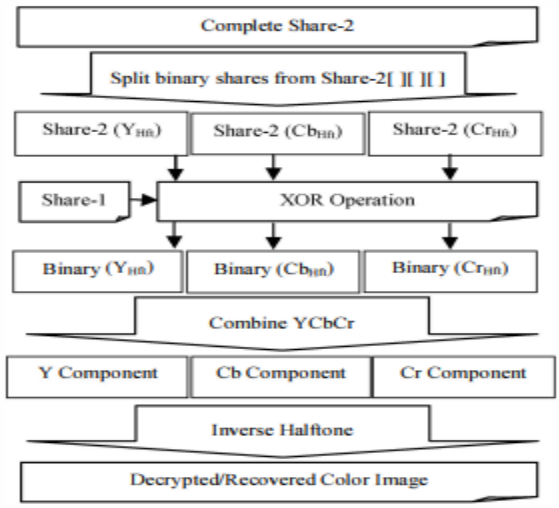

Fig. 3. Flow of decryption technique

V. CONCLUSION

In this research, we introduced a medical data encryption technique based on natural picture cryptography. This novel technique generates key and cypher with efficient calculation. The area required to store the basic passkey image and cypher picture is less than that required to store the original encrypt image. The image's pixel remained unchanged throughout the procedure. With this procedure, the image appearance of the restored image is satisfactory. Because of its resistance to a limited number of cryptographic, it may be adapted to operate for identity image-based encryption.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology - EUROCRYPT'94, A. D. Santis., Ed., vol. 950. SpringerVerlag, 1995, pp. 1-12.

[2] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary versionappears in "Security Protocols", M.

Lomas ed. Vol. 1189 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1997, pp.197-202.

[3] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416-428.

[4] E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." Designs, Codes and Cryptography, 11(2), pp.179-196, 1997.

[5] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, lEICE, 2008

[6] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, 2008, pp. 252-256.

[7] Wen-Pinn Fang, "Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[8] Zhengxin Fu, Bin Yu, "Research On Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce, 2009, pp 533-536.

[9]. Amandeep Kaur and Satveer Singh, "A hybrid technique of cryptography and watermarking for data encryption and decryption", IEEE, Punjab, India, 2016.

[10]. Jai Singh, Kamil Hasan and Ravinder Kumar, "Enhance security for image encryption and decryption by Appling hybrid techniques using MATLAB", IJIRCCE, vol.3, issue 7, July 2015.

[11]. Pooja Rani and Apoorva Arora, "Image security system using encryption and steganography", IJIRSET, vol.4, issue 6, June, 2015.