International Journal of Innovation Engineering and Science Research

Open Access

Combining of Cryptography and Steganography for Improving of Security

Muharrem Tuncay Gençoğlu
Department of Computer Technology, Firat University
Elazig, TURKEY

Sarhad Baez Hasan
Department of Software Engineering, Firat University
Elazig, TURKEY

ABSTRACT

To hide hidden data in digital images, a variety of techniques are available, some of which are more complex than others. Public key cryptography is very useful for applications, and the technique used depends on the requirements for encryption and encryption data. Hiding is a kind of hiding method in which the host image is exactly retrievable. Presence lossless makes this technique suitable for medical and military applications. The image pixels are replaced with additional data into new values to embed several data pixels by S-block at multiple layers. From the original image, the embedded data can be extracted and the original image can be recovered from the decrypted image directly. Embedded data can be extracted directly from the encrypted domain. The decryption of the original plaintext image doesn't affect the data embedding operation. With the combined technique, before decryption, a receiver may extract a part of embedded data, and recover the original plaintext image after decryption. A slight distortion is introduced due to the compatibility between the lossless and reversible schemes. The data embedding operations can be performed in the two manners simultaneously performed in an encrypted image and decrypted image. In this thesis, the design of Caesar cipher and Vigenere cipher is presented. Block 4 provides good encryption properties and software productivity. The proposed technique for the design of the S-box chain chaos provides a very secure level. The result of the implementation shows that the proposed method is suitable for lightweight cryptography due to the use of low resources using the C # .Net implementation tool.

Keywords—*Image encryption, Lossless data hiding, data hiding, Public key encryption, Caesar cipher etc.*

I. INTRODUCTION

These days security is the most basic factor in any correspondence framework. Issues in such security frameworks are trustworthy in protection's verification and non-disavowal; such issues should be dealt with deliberately. The security objectives are specific: classification of the accessibility and honesty that can be debilitated by security assaults. Hence, to ensure the first data from such assaults the information concealing procedures are actualized. Reversible Data Hiding (RDH) systems are connected to steganography and cryptography capacities for the purpose of looking after security and verification [3]. Encryption and information covering up are two methods of information security. Concealing procedures insert unique information which we wouldn't prefer to reveal into cover media by presenting satisfactory slight adjustments while encryption strategies convert plaintext information into mixed up frame i.e. ciphertext. It is valuable to insert the information into an advanced media to convey the mystery messages. The proprietor can alter the first content of the utilizing media pictures, so that the implanted information is hidden. [1] Encryption gives classification for pictures and videos; it is also a successful system which changes over the first and mystery information to an immense one.

II. General Review of Cryptography and Steganography

Many researchers believe that security is considered as the most critical factor in any communication systems. Issues in such security systems are integrity, privacy, authentication and non-repudiation; it should be handled carefully. Here the security goals are namely: confidentiality, availability and integrity that can be threatened by security attacks. Thus, to protect the original information from such attacks the data hiding techniques are implemented. Boghdad et al [1] believed that the information on the images has brought a lot of enthusiasm with the use of systems of impotence or immobilization. Despite the fact that miserable systems can create widespread concealment, a high-resolution image cannot be recovered. The number of applications needs to restore the correct image of the host; for example, medications can be installed quietly without knowing the medication picture. Using the hidden methods of unparalleled information, the restriction is limited because the host image should be preserved. In this paper, a pressure-free installation system is proposed. In this way, image histograms detect that they detect the limitations of installing different photos. The Maxima and Minima histograms are used in placing limited estimates. The proposed system provides a hidden border that can match up to half the size of the host image for wide-area images (similarly).

Tian [2] investigated on a case study to enter the layout installation methods in a distinctive image. They have not come up with a separate image for another image that has been placed on another layer unless the current image has any contrast enhancements. The burden of these procedures is that the image quality may be very corrupt, even before it installs the next layer, considering the fact that placing the last layer uses any expandable contrast, including ones they are very intense. Based on the total number of Haar waveforms, we propose that we install another DE calculation, which uses the flat as the vertical contrast images to cover the information. We present a tracking and dynamic distinction section now. The system even shoots low-contrast photos in two different images and dramatically avoids the situation, with the largest contrast in the primary contrast image being used, while there's almost no option for low contrast adjustment. There is no second image.

GENÇOĞLU (2017) [31] shows the linking cryptography with steganography, a diverse cryptographic way is introduced by using power sequence convert, codes of ASCII and science of steganography. In this perspective, he created a new algorithm for cryptology, he adapted extended Laplace alert of the exponential duty for encrypting the basic text and he used codes of ASCII for sustaining the privacy of the hypertext Alert. Chipertext has fixed by steganography technique in another main text to cover the being of chipertext. For encryption, he displayed the equivalent converse of power sequence alert.

For the purpose of maintaining the security and authentication, Reversible Data Hiding (RDH) techniques are related to steganography and cryptography function. Encryption and data hiding are two techniques of data protection. Data hiding techniques embed original data which we don't want to disclose into cover media by introducing slight acceptable modifications; while encryption techniques convert plaintext data into unreadable form i.e. ciphertext. It is beneficial to embed the data into digital media to communicate the secret messages. The owner can modify the original content of the media using images so that the embedded data is hidden. Encryption provides confidentiality for images and video as well as it is an effective technique which converts the original and secret data to incomprehensible one.

III. TAXONOMY & ARCHITECTURE

A. Reversible Data Hiding

Reversible or lossless information concealing systems shroud information in a host motion (for instance, a picture) and permit extraction of the first host flag and furthermore the installed message. There are two imperative necessities for reversible information concealing systems: the inserting limit ought to be substantial, and bending ought to be low. These two necessities are fighting each other.

When all is said to be doing your work, a higher level of implanting will cause a high level of twisting. An enhanced strategy inserts a similar limit with bring down twisting or the other way around.

Tian's distinction extension system already had the most elevated installing limit and the least contortion in picture quality. His strategy separates the picture into sets of pixels and uses each genuine match for concealing one piece of data. Along these lines, his implanting limit is best case scenario 0.5 b/pixel. The joined utilization of the rhombus expectation conspires, arranging, histogram move technique, and, subsequently, little size of area delineate generally better outcomes looked at than existing plans.

Information covering up, frequently alluded to as computerized watermarking, has as of late been proposed as a promising strategy for data affirmation. Inferable from information stowing away, notwithstanding, some perpetual twisting may happen and subsequently the first cover medium will be unable to be turned around precisely even after the concealed information have been separated out. Following the arrangement of information pressure calculations, this kind of information concealing calculations can be alluded to as lossy information covering up. It very well may be demonstrated that the greater part of the information concealing calculations announced in the writing are lossy. Here, let us inspect three noteworthy classes of information concealing calculation. With the most prevalently used spread-range watermarking systems, either in DCT space or square 8x8 DCT areas, round off blunder as well as truncation mistake may occur amid information implanting. Therefore, there is no real way to invert the stego media back to the first without mutilation. For the slightest noteworthy piece plane (LSB) inserting techniques, the bits in the LSB are substituted by the information to be implanted and the bit-substitution isn't retained. Thus, the LSB strategy isn't reversible. With the third gathering of much of the time utilized watermarking procedures, called quantization file tweak (QIM), quantization blunder renders lossy information covering up.

In applications, for example, in law implementation, medicinal picture frameworks, it is wanted to have the capacity to turn around the stego-media back to the first cover media for legitimate thought. In remote detecting and military imaging, high precision is required. In some logical research, test information is costly to accomplish. Under these conditions, the reversibility of the first media is wanted. The information concealing plans fulfilling this prerequisite can be alluded to as lossless. The terms of reversible, or invertible are additionally utilized much of the time. These procedures, similar to their lossy partners, embed data bits by altering the host flag, along these lines prompting an inserting bending. All things considered, they likewise empower the evacuation of such twists and the correct lossless-reclamation of the first host motion after extraction of installed data.

One of the main elements of this algorithm is that it is based on a piecewise theory. In other words, in each region, the central vector orientation of the center is determined by all the pixels in that area. As a result, the algorithm is a certain amount of compression of the image. Another key element of this algorithm is that it uses the plugin modulo-256 to prevent overflow and the following flow, so it has reversibility. As a result, however, as mentioned, this algorithm suffers from salt and pepper noise. In the stoical medical image, the intense noise of salt and pepper is clear. PSNR The stego image is less than 10dB compared to the original image, while 476 bits of information are embedded in this 512x512 image. Not only for medical imaging, salt noise and pepper may also be intense for color images. We applied this algorithm to eight JPEG2000 color test images. There are four of eight pictures that suffer from intense salt and peppery noise, while four others experience less intense pepper noise. PSNR can be as low as less than 20 dB when there is intense noise when 1412 bits of information are embedded in a color image of 1536x1920x24. From the above, it can be concluded that all the hidden algorithms of reversible data are based on the incremental modulo-256 to prevent overflow and downstream flow, and cannot be applied to many real applications, and from this, it should be avoided.

B. Flexible data technique with room reservation before encryption

In the previous method, the data embedded can be available without any error after the decryption of the encoded data. But the cover that is the image which contains the data cannot be effectively rebuilt. That is the major drawback of the framework mentioned previously.

a. Generation of Encrypted Image

To create a coded image, the initial stage can be divided into three stages: image packaging, auto-reversal installation after photo encryption. To the beginning, the stage of the image step divides the first image into two parts An and B. At that moment, LSBs come from A inversely to B using Rambo justification calculations, with the goal that LSBs use A to retrieve messages.

b. Image Partition

The supervisor is here to save the room before encoding a standard RDH system, so the packaging goal is to create a normal B region in which the Rambo computing method can perform better. To do that, without loss of consensus, accept the first picture C is a dim scale picture with its size M x N, it is isolated into two equivalent measured pictures. In this, the B part has the smoother region to apply the RDH procedure. The LSBs of the pixels of A where the information is stowing away is put away.

c. Self-Reversible Embedding

The objective of self-reversible inserting is to implant the LSB-planes of an into B by utilizing the basis rhombus calculation.

d. Image Encryption

In the wake of revamping self-inserted picture and saving rooms, the encryption is finished with the assistance of encryption key. It is an 8-bit key. In this, the encryption is finished by XORing the picture with the key. At last, we insert 10 bits data into LSBs of initial 10 pixels in encoded rendition of A to tell the information hider the number of lines and the number of bit-planes he can implant data into. After picture encryption, the information hider or an outsider can't get to the substance of unique picture without the encryption key, consequently, the security of the substance proprietor is ensured.

e. Data Hiding In Encrypted Image

Once the information hider secures the scrambled picture, he can implant a few information into it, despite the fact that he doesn't gain admittance to the first picture, The inserting procedure begins with finding pixels in which the information can implant in the scrambled adaptation of picture. Since the information hider has the areas where the information can be installed it is easy for the information hider to peruse bits data in LSBs of encoded pixels. Subsequent to knowing what number of bit-planes and lines of pixels he can alter, the information hider just receives LSB substitution to substitute the accessible piece planes with extra information. At long last, the information hider encodes as indicated by the information concealing key to defining scrambled pictures containing information.

f. Data Extraction and Image Recovery

Since information extraction is totally free from picture decoding, the request of them infers two diverse down to earth applications. To oversee and refresh individual data of pictures which are encoded for ensuring customers' security, a sub-par database supervisor may just gain admittance to the information concealing key and need to control information in the scrambled space. The request for information extraction before picture decoding ensures the practicality of our work for this situation. At the point when the database administrator gets the information concealing key, he can decode the LSB-planes of An and remove the extra information by straightforwardly perusing the unscrambled adaptation. While asking for refreshed data of scrambled pictures, the database administrator, at that point, refreshes data through LSB substitution and encodes refreshed data as indicated by the information concealing key once more. As the entire procedure is totally worked on the scrambled area, it maintains a strategic distance from the spillage of unique substance.

C. Data Hiding and Image Encryption

The procedure of information covering up and picture encryption in this technique is completed in four stages. Be that as it may, before the procedure starts, the sender's sign into the application utilizing a substantial client id and a secret phrase. This GUI is given to guarantee a higher level of security even before the genuine procedure starts. Therefore, with such high security there stays just a little line for an interloper to sniff into the exchange. The procedure of real information covering up and encoding the pictures alongside inserting them with information is as per the following. In the initial step, the picture chosen by the sender is partitioned into three shades. These shades are disintegrated so that we get decayed picture segments as Red, Green and Blue. These decayed pictures frame RGB plane for every one of the segments, in this manner bringing about the principal plane being the red plane, the second the green plane and the third the blue plane. So the determination is that a shading picture is shaped by stacking the three planes together, similar to a sandwich. The second step is saving room before encryption for the information. The principal stage can be isolated into two stages: the picture parceling and self-reversible implanting. At first, the picture parcel step isolates the blue plane of the first picture picked by the sender, into two sections say A and B; at that point, the LSBs of An are reversibly installed into B with a standard RDH calculation utilizing addition so LSBs of A can be utilized for obliging messages. Presently, the last stage is known as picture encryption. Here at this stage, we utilize Algorithm Encryption Standard (AES Algorithm) to encode the picture for secure exchange over the system. It encodes the first picture pixel esteems with encryption key esteem. We utilize an open key encryption technique to create the keys. The last stage is concealing the information in scrambled pictures. Subsequently in the wake of having what number of bit-planes and the lines of the pixels the information hider or sender can adjust, the information hider consequently basically utilizes a side-coordinate forecast technique or just a LSB substitution way to deal with swap the accessible piece planes with extra information that he expects to send safely without making it defenseless against dangers. In the side-coordinate forecast approach, the histogram is made by misusing the distinction in every one of the qualities among pixels and their prescient qualities. All prescient mistake esteems are changed into histograms to make higher pinnacle esteems. In the extraction and turning around the process, the side-coordinate forecast is connected to the stego-picture, and the made histogram is handled for extraction and switching. At long last, the information hider sets a name following 'n' to bring up the end position of the installing procedure and further encodes 'n' as per the information concealing key to figure the stamped scrambled picture.

D. Pre-Process for Complete Recovery

In the previously mentioned calculation, it is necessitated that all pixels checked in are inside. In the event that there is any bouncing pixel esteem (0 or 255), flood or sub-current will be caused by histogram moving. To maintain a strategic distance from it, the histogram should be pre-handled preceding the histogram adjustment activities. In particular, the pixel estimations of 0 and 255 are adjusted to 1 and 254, separately. Hence, no flood or undercurrent will be caused in light of the fact that the conceivable difference in every pixel esteem is to retain the pre-prepared pixels, an area outline indistinguishable size from the first picture is produced by allocating 1 to the area of an altered pixel, and 0 to that of an unaltered one (counting the 16 prohibited pixels).

E. Contrast Enhancement

Every one of the two tops in the histogram is part into two contiguous canisters with comparable or same statures in light of the fact that the quantities of 1s in the message bits are required to be relatively equivalent. To build the concealing rate, the most noteworthy two containers in the adjusted histogram are additionally been part by applying Eq. (1) to all pixels checked in the histogram. A similar procedure can be rehashed by part every one of the two crests into two contiguous canisters with comparable statures to accomplish the histogram evening out impact.

F. Data Hiding For JPEG Images

This paper proposes a lossless information concealing method for JPEG pictures in light of histogram sets. It inserts information into the JPEG quantised 8x8 square DCT coefficients and can accomplish great execution as far as PSNR versus payload through controlling histogram sets with ideal limit and ideal district of the JPEG DCT coefficients. It can acquire higher payload than the earlier expressions. What's more, the expansion of JPEG document measure after information inserting stays unnoticeable. These have been confirmed by our broad tests.

G. Digital Image Water Marking

Watermarking, which have a place with the data concealing field, has seen a considerable measure of research intrigue as of late. There is a great deal of work starting to be directed in various branches in this field. Steganography is utilized for mystery correspondence, though watermarking is utilized for content assurance, copyright administration, content verification and alter recognition. In this paper, we present a definite review of existing and recently proposed steganographic and watermarking procedures. We group the systems in light of various areas in which information is installed.

H. Digital Image Steganography

In basic terms, steganography can be characterized as the workmanship and study of undetectable correspondence. This is refined through concealing data in other data, subsequently concealing the presence of the imported data. In spite of the fact that the idea of steganography and cryptography are the same, steganography contrasts from cryptography. Cryptography centers around keeping the substance of a message mystery, steganography centers around keeping the presence of a message mystery. Steganography and cryptography are both approaches to shield data from undesirable gatherings however neither innovation alone is impeccable and can be endangered. Once the nearness of concealed data is uncovered or even suspected, the reason for steganography is halfway vanquished. The quality of steganography would thus be able to be intensified by joining it with cryptography.

IV. PKC (Public-Key Cryptography)

Whitfield Diffie, Martin Hellman and Ralph Merkle presented an altogether extraordinary kind of figure in 1976. In these cryptographic frameworks, encryption and decoding utilize two distinctive keys i.e. one is an open key, known to everybody and other is a private key which is just known to the beneficiary of the message. At the point when sender A needs to communicate something specific safely to beneficiary B, he utilizes the general population key of B to encode the message. Beneficiary B at that point utilizes her private key to unscramble the message. Uneven calculations are prevalent for traditional information encryption as well as for application, for example, computerized marks and key foundation.

A. Least Significant Bit Based Steganography

It is the most popularly and commonly used approach for data hiding scheme where data is hidden in the least important part of the image. It is the simplest steganographic method where secret information is hidden in a subset of the LSB plane of the image. This method is the easiest and simplest and yet very effective way of hiding information in an image. In this method, the LSB of each pixel value in the cover image is used to hide the MSB of another image. It is assumed that LSB of the image is the non-important value which does not impact the appearance of the image. There are various steganographic tools available like S-Tools 4, Steganos and StegoDos, which implement LSB replacement in the spatial domain. This approach works by substituting duplicate values of the image with secret information. The embedding process involves a cover image in which substitution is done to hide information. This method works with a grid of pixels (raster image) which are used without compression (*.gif, *.bmp). *.GIF, *.BMP are more preferred file formats as they involve lossless compression. Along with *.gif, *.bmp, other image formats are used as cover images. Lossless compression is used because it maximises the embedding capacity of the image. Using the least

significant bit technique to hide the data, both invisibility and reasonably high storage payload is achieved

B. Proposed Chaotic Image Encryption Algorithm

The calculation that can be utilized to create n-bit x nbit S-boxes essentially works by changing over the yields of disordered frameworks into whole numbers somewhere in the range of 0 and 2n. The calculation's task is given underneath: Algorithm

Step1: System directions are gotten by explaining the partial disorganized Lorenz framework with chose introductory conditions and confused parameter esteems utilizing.

Step2: Select four parameters, base-ten esteem meant by these digits is changed over into whole numbers somewhere in the range of 0 and 2n by taking the modulus of this number at mod (2n).

Step3: S-Box is produced utilizing the codes relating to yields with the code comparing to the littlest yield being the main cell of the S-Box.

Step4: The got number is added to the table on the off chance that it isn't now present; generally the procedure returns to Step 1 to produce another whole number esteem.

Step5: The procedure goes ahead until the point that all cell esteems are filled.

Step6: After the S-Box is produced; we have applied the relative change to every component of our riotous S-boxes components xT = [x0, x1, x2, … , x7] T , i.e.;

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

(1)

Step7: We have connected S-box change on the got S-encloses Step 6 for picture encryption.

CONCLUSION

In the lossless program, the installed information can be specifically separated from the encoded space; the task of placing information on the encryption does not affect the first plain text file. In the reversible layout, additional information can be removed from plain text space, and although the slight bending in the decoding image is provided, the first simple image can be restored without any fault. Given the similarity of the two programs, the tasks of inserting data from irreversible and irreversible programs can be done while encoded in the image. Along these lines, the receiver may separate a piece of information entered in the coding area and focus on another piece of information installed and reconstruct the first simple text file in plain text space. A safe encryption and Caesar figure implanting plan in view of change dissemination engineering has been proposed. Additionally, by utilizing the novel proposed strategy for installing the information, the extent of the net payload can be expanded adequately. That is, we can shroud enough information into the encoded picture and furthermore look at the execution of the current strategy and proposed technique pictures regarding parameters like PSNR esteems information limit, size of the cover picture and so on. In our plan, both the pixel level and bit level stage are supplanted by square change and the S-square guide is utilized to process each square in such a route in this way, to the point that its key space can be moved forward. It includes pseudorandom number age in light of various keys and utilizes coordination's maps for dissemination Reproduction results demonstrate that acceptable security execution is accomplished in just a single encryption round itself. The proposed conspire is checked by the

security examination on its key affectability, arbitrariness test, factual and differential properties and is reasonable for continuous application.

ACKNOWLEDGMENTS

Before going into details, I would like to give my gratitude to Almighty Allah for granting me the ability to finish this report that will hopefully lead to me going on to do a Master's degree. In addition, I want to honour.my supervisor Assist. Prof. Dr. Muharrem Tuncay GENÇOĞLU for his warm support and guidance whilst working on this project. This will be my first step towards a Master's degree and is the beginning of a project and ideas that have been piled up in my mind for years. I highly regard this field to work in and it marks my professional career. Moreover, I appreciate my previous instructors who made me consider a new and different field. This paper is going to mark my knowledge about a new invention of information security by displaying, making and solving some principles of the field and adding one more branch to the tree of the computer world.

REFERENCE

[1] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.

[2] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing, 14(2), pp. 253–266, 2005.

[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.

[6] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible Data Hiding in Encrypted Images by reserving Room before encryption", IEEE Trans. On information forensics and security, vol,8 No.3, March 2013.

[7] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers" vol. 21, no. 6, pp. 2991–3003, June. 2012.

[8] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, December.2011.

[9] L. Luo et al., "Reversible image watermarking using interpolation," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–G. Xuan, J. Chen, J. Zhu, Y.Q. Shi, Z. Ni, and W. Su, "Lossless Data hiding.

[10] I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.

[11] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. on Information Forensics and Security, vol. 8, no. 3, pp. 553-562, Mar. 2013.

[12] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography," IEEE Trans. on Circuits and Systems for Video Technology, 2015.

[13] J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.

[14] Z. Qian, and X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.

[15] X. Cao, L. Du, X. Wei, et al., "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Trans. On Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.

[16] W. Hong, T. Chen, H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199- 202, Apr. 2012.

[17] Alka Dileep, K.Anusudha, Muhammed Asad P. T., " An Efficient Reversible Data Hiding Technique in Encrypted Images Based on Chaotic Map," IEEE International Conference on Control Instrumentation, Communication and Computational Technologies, 2015.

[18]. Rintu Jose, Gincy Abraham "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance" IEEE International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013), DOI:10.1109/AICERA-ICMiCR.2013.6576038, Pages:1-5

[19]. Zhenxing Qian, Xinpeng Zhang, Guorui Feng "Reversible Data Hiding in Encrypted Images Based on Progressive Recovery" IEEE Signal Processing Letters, DOI:10.1109/LSP.2016.2585580, Volume: 23, Issue: 11, Nov. 2016, Pages:1672-1676

[20]. Shuang Yi, Yicong Zhou "An Improved Reversible Data Hiding In Encrypted Images" Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on, DOI:10.1109/ChinaSIP.2015.7230396, Pages:225-229

[21]. Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo "Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting" Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on, DOI: 10.1109/ICASSP.2016.7472053, Pages:2129-2133

[22]. Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography" IEEE Transactions on Circuits and Systems for Video Technology, DOI:10.1109/TCSVT.2015.2433194, Volume: 26, Issue: 9, Sept. 2016, Pages:1622-1631

[23] X. Hu, W. Zhang, X. Li, N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. On Information Forensics and Security, vol. 10, no. 3, 653-664, Mar. 2015.

[24] W. Zhang, X. Hu, N. Yu, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," IEEE Trans. on Image Processing, vol. 24, no. 1, pp. 294-304, Jan. 2015.

[25] Ioan-Catalin Dragoi, Dinu Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014.

[26] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, pp. 118-127, Jan. 2014.

[27] Wu J, Zhang R eta. Reliable Detection of BPCS Steganography [J]. Journal of Beijing University of Posts and Telecommunications, 2009, 32(4): 113-121

[28] ZHANG H L, ZHANG X Y. A secure BPCS steganography against statistical analysis[C]. 8th International Conference on Signal Processing. 2006: 990-992.

[29] Arti Yadav, Minaxi Doorwar "Novel Framework for Improving Embedding Capacity of the System using Reversible Data Hiding Technique" July 2015

[30] Veena S. Nair , Dhanya K. Sudhish " Lossless and Reversible data hiding in Encrypted Images" Feb 2017.

[31] GENÇOĞLU, M. T. (2017). Combining Cryptography with Steganography. Second International Conference on Computational Mathematics and Engineering Sciences(CMES) (p. 16). Istanbul: CMES2017.

[32] GENÇOĞLU, M. T. (2017). Programming Encryption Algorithms with Steganography. International Conference on Engineering Technology and Innovation (ICETI). Sarajevo: ICETI 2017.

[33] Shweta Patil Student, Electronics Amrutvahini college of engineering, Sangamner Maharashtra, India, "Data Hiding Techniques: A Review" International Journal of Computer Applications (0975 – 8887) Volume 122 – No.17, July 2015.