International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Encryption and Authentication of Effigy by using SVD

Komal Gaikwad[1], Kshitija Kurnawal[2], Dhanashri Padase[3], Deokate S.T.[4], Salve B.S.[5]
[1, 2, 3, 4]*Student, Computer Engineering, SBPCOE Indapur, Maharashtra, India*
[5]*Assistant professor, Computer Engineering, SBPCOE Indapur, Maharashtra, India*

Abstract: ***Day by day, data broadcasting over internetworking is accelerating tremendously. As we see lot of data is abducted over network, so it necessitates providing data security. The RDH (Reversible Data Hiding) approach is intended for grayscales images previously and it cannot be directly applied to the palette image. Here, at the sender side the palette image is used as input and the encryption of image is done by using the encrypted key. In the image, alterations are done by using the color partitioning with RGB model. DWT (Discrete Wavelet Transform) is used for hiding textual data into multimodal image. After performing the encryption of the intended image, some data is hidden by utilizing data hiding key. At receiver side the received image is decrypted and the result is identified. The original contents can be reconstructed after data extraction and the contents of owners privacy remains protected.***
Keywords: Encryption, palette image, color partitioning, DWT.

I. INTRODUCTION

In this system, proposed a reliable SRDH scheme for encrypted palette images. The proposed method aims to divide the palette colors into multiple color triples,
among which the embeddable color-triples are recorded and self-embedded into the encrypted index matrix together with some other auxiliary data before the image transmission so that, secret bits can be carried by altering the pixel values of embeddable color-triples on the data hider side.SVD stands for Singular Value Decomposition. SVD method can transform matrix A into product (USV) which allows
us to refactoring a digital image in three matrices. The using of singular value of such refactoring allows us to represent the image with a smaller set of values which can preserve useful feature of original image but useless storage space in the memory and achieve the image compression process. In proposed system we have used DWT (Discrete Wavelet Transform) to hide textual data into multimodal image. Discrete Wavelet transform (DWT) which transforms a discrete time signal to a discrete wavelet representation. It is based on time scale representation which provides efficient multi resolution and DWT operates at maximum clock frequency 99.197MHZ respectively. After that a receiver acquires the encrypted and marked image, receiver should extract the self-embedded auxiliary
Data at first. The subsequent procedure depends on the role of the receiver. If receiver has only the data hiding key, receiver can retrieve the hidden data without knowing the image content. Receiver can decrypt the marked and encrypted image with a good image quality. If the receiver has both the data hiding key and encryption key, receiver can not only retrieve the hidden data, but also recover the image without loss.

II. LITERATURE SURVEY

The two new invertible watermarking systems for authentication of digital images in the JPEG format. The first technique is based on damage free compression of biased bit-streams derived from the quantized JPEG coefficients. The second technique modifies the quantization matrix to enable damage free embedding of one bit per DCT coefficient. This two techniques are fleet and can be used for general distortion-free (invertible) data embedding. The further focus on extending the methods to the MPEG-2 format [1].
Reversible data embedding has drawn lots of fondness opportunity recently. The original digital content can be completely revived. In proposed system [2] a novel reversible data embedding method for digital images. The system explores the redundancy in digital images to derive very high embedding capacity, and keep the distortion low. The only Gray scale image distortions are low and derive the very high embedding capacity. The future work is for difference expansions for a colorful image.
Reversible data hiding algorithm, which can retrive the original image without any distortion from the marked image after the latent data have been extracted. This lower bound of PSNR is greater than that of all reversible data hiding techniques reported. The computational complexity is low and the enforcement time is short. This technique [3] frequently used images, medical images, Texture images, Aerial images and they represents the histogram of an image.

The reversible or lossless watermarking algorithm for effigy without using a location map in many cases. This algorithm employs estimate errors to embed data into an image. The performance of the proposed reversible watermarking plan is evaluated using different images and compared with methods of Kamstra and Heijmans et al. these result avowedly indicate that the embed more data with less distortion [4].

The integer convert based reversible watermarking is proposed. The system 1st show that Titan's variation expansion (DE) technique can be reformulated as an integer convert and other is establishing the payload dependent place map which occupies a little payload. The system [5] Tian's DE technique uses to viewpoints of reversible watermarking. Furthermore, selected the block with better expandable based on misuse estimation function.

A new blind authentication method based on the confidential sharing technique with a data refit capability for grayscale document images via the usage of the Portable Network Graphics (PNG) image is proposed. In the process of image authentication an image blocked is marked as tampered. Information repairing is then applied to each tampered block by a reverse Shamir scheme after connecting two shares from unmarked blocks. Measures for protecting the safety of the data hidden in the alpha channel are proposed. For more studies may be directed to choices of other block sizes just like a prime number, coefficient covert sharing etc. to better the data repair effects [6].

The SVD is not efficient transforms in Image Processing application. SVD properties for images are experimentally presented to be utilized in developing new SVD based image processing application [7].SVD in image processing and identify important various applications and open research directions in this increasingly important area; SVD based image processing in the future research.

The two-dimensional discord histogram changes are based on a novel reversible data hiding (RDH) scheme is proposed by utilizing difference-pair-mapping (DPM). By considering each pixel-pair and its reference, a precede consisting of pairs of contrast values is enumerated a two-dimensional variance-histogram is generated by counting the frequency of the resulting contrast-pairs [8]. In addition of this system a pixel pair choice strategy is used to further enhancement of embedding performance.

The novel method by consumption reserving room early encryption with a universal algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can derive real reversibility, that is, data extraction and effigy recovery are free of any error [9]. The further improvement on the quality of marked decrypted image.

In proposed system [10] technique for authentication of effigy with self-repair capability for fixing tampered image data is explained. Alpha channel is assembling in the greyscale image. Authentication signal is calculated by using binary image and embedded in the alpha channel to originate an authentic image. After embedding the authentication signal, image is encrypted and the stego-image is detected. Then data is repaired at the pixel level by using reverse secrete sharing scheme and secret image can be recovered without any damage. Now days poly digital documents are shifted on the internet regularly e.g. circuit diagrams, signed documents, etc.

The authentic effigy is encrypted at sender side and receiver side this image is decrypted. The embedded authentication signal is extracted from the received authentic effigy. The new authentication signal is determined by the binary image of the received authentic image. New authentication signal is paragon with the extracted signal then the integrity check is provided. The tampering of data is detected successfully without any original image backup [11]. The result is provided only for the grayscale images and supposed to spread for color images as well.

For better explore the correlation between neighbor pixels, we propose to consider the patch-level sparse representation when hiding the confidential data. The widely used rare coding technique has demonstrated that a patch can be sequentially represented by some atoms in an over-complete dictionary. In this method HC-SRDHEI method which inherits the merits of RRBE and the separability property of RDH system in encrypted image [12].Further in the mighty representation of sparse coding, a big vacting room can derived and this the data hidder can embedded more confidential message.

RDH into encrypted images is increasing and regarding to researchers as the inherent thing can be correctly reconstruct after the embedded data are extracted while the thing owner's secrecy remains secured. The existing RDH techniques are designed for grayscale images and cannot be straight applied to palette images. In this system we will use the encryption key and data hiding key at the sender side for encryption of image and at the receiver side the decryption is complete and original image is obtain. The system can be spread for video marking [13].

III. PROPOSED SYSTEM

This proposed system is used to move message from sender to receiver with security .To protected this data from unauthorized users,we are developing a system using the Encryption,decryption and Data Hiding key. In this system colorful effigy(palette) is considered.The palette image means colorful effigy which is used as input at the sender side.Palette will be encrypted and after that the image data will be covert into the image using data hiding technique . At receiver side data is getting extracted by giving keys that are the data hiding and image will be decrypted by using decryption key.At the last stage we will try to gain original image with high infallibility.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

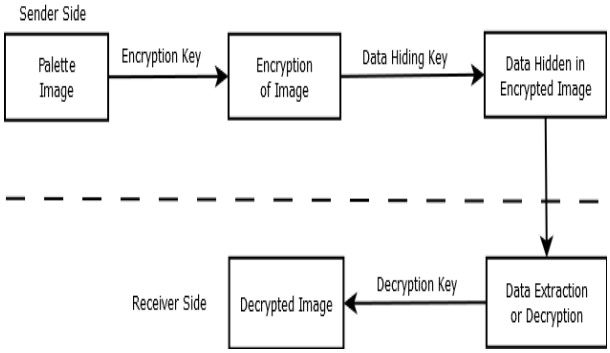


Fig. 1 Proposed System Architecture

IV. ALGORITHMS

In the proposed system three algorithms are used.

A. Singular Value Decomposition (SVD) Algorithm

In this proposed system SVD algorithm used for encryption process. SVD method can transform matrix A into product (USV) which allows to refactoring a digital image in three matrix. The using of singular value of refactoring allows us to represent the image with a smaller set of values which can preserve useful features of original image but useless storage space in the memory and achieve the image compression process. After decryption of image gain better quality of image due to SVD.

1) Algorithm

a) Step-1: Read the image (input image).

Syntax: img=imread('filename.jpg');

b) Step-2: Split the input image (colour image) into R, G, B channels.

Syntax:

Red = img (:,:, 1);

Green = img (:,:, 2);

Blue = img (:,:,3);

c) Step-3: Decompose each component using Singular Value Decomposition

Syntax: u,s,v=svd (I);

Step-4: Select r value and discard the diagonal value of S matrix not required. Construct the image using the selected singular values.

Syntax:

For j=1:r

c=c+s (j,j)*u(:,j)*v(:,j).';

end

The R-value in the m-file represents the number of iterations taken on each layer used in the resulting decomposition. This is actually the rank of the SVD matrix. By increasing the rank we can increase clarity until an optimal image is reached.

d) Step-5: Display the compressed image.

B. RSA Algorithm

Ron Rivest, Adi Shamir and Len Aldeman have developed this algorithm (Rivest- Shamir-Aldeman) in 1978.It is a public key encryption algorithm. It is block-cipher which converts plain text into cipher text at sender side and vice versa at receiver side.

1) Algorithm

a) Step-1: Generate two large random primes, p and q, of approximately equal size such that their product n=pq is of the required bit length, e.g. 1024 bits.

b) Step-2: Compute n=pq and = (p1)(q1).

c) Step-3: Choose an integer e, 1¡e¡, such that gcd (e,)=1.

d) Step-4: Compute the secret exponent d, 1¡d¡, such that ed1mod.

e) Step-5: The public key is (n,e) and the private key (d,p,q). Keep all the values d, p, q and secret. [Sometimes the private key is written as (n,d) because you need the value of n when using d. Other times we might write the key pair as ((N,e),d).]

where,
n is known as the modulus.
e is known as the public exponent or encryption exponent or just the exponent.
d is known as the secret exponent or decryption exponent.

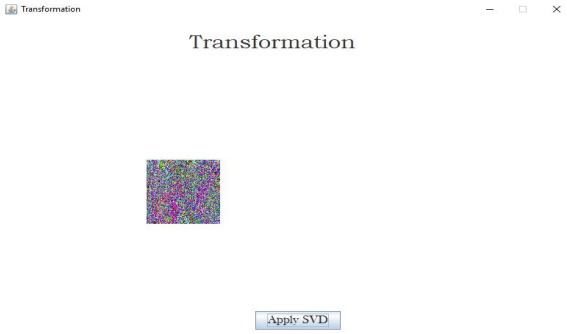
C. *Discrete Wavelet Transform (DWT) Algorithm*

In proposed system we have used DWT (Discrete Wavelet Transform) to hide textual data into multimodal image. Discrete Wavelet transforms (DWT) which transforms a discrete time signal to a discrete wavelet representation. It is based on time scale representation which provides efficient multi resolation and DWT operates at maximam clock frequency 99.197MHZ respectively.

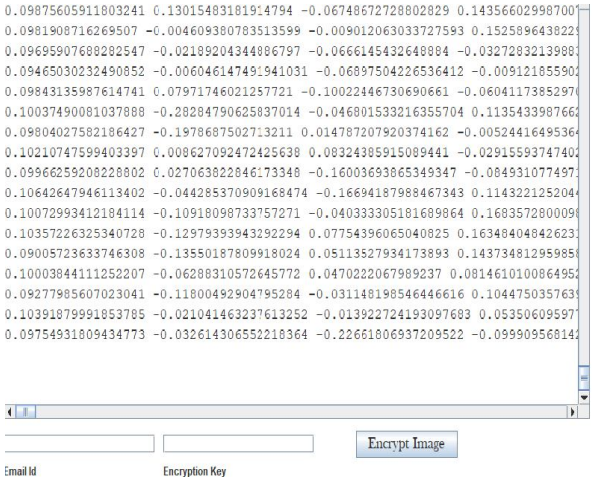
V. RESULT

A. *Input Image Taken From User*

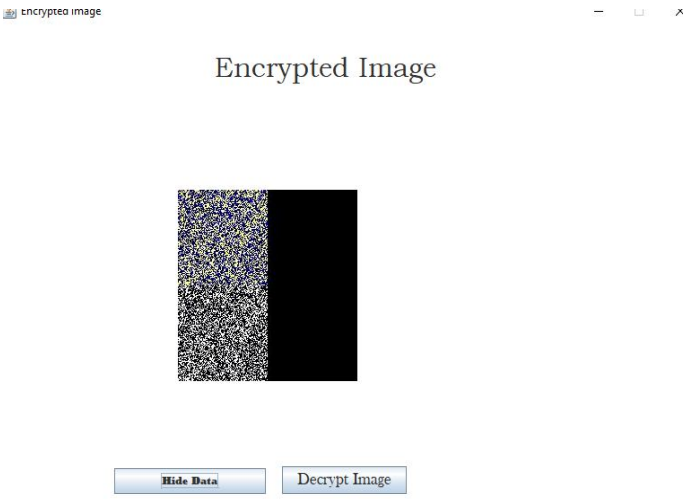
B. *Convert into Gray scale Image*



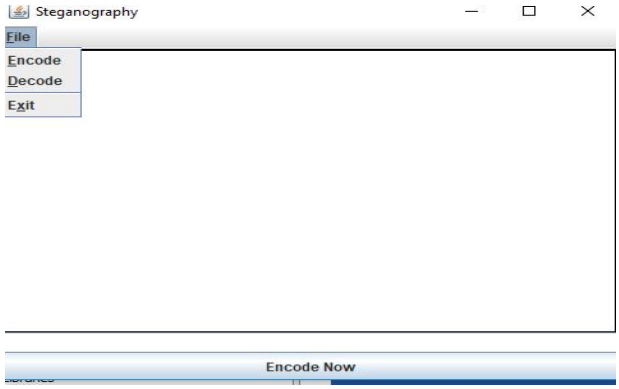
C. *Applied SVD Algorithm*



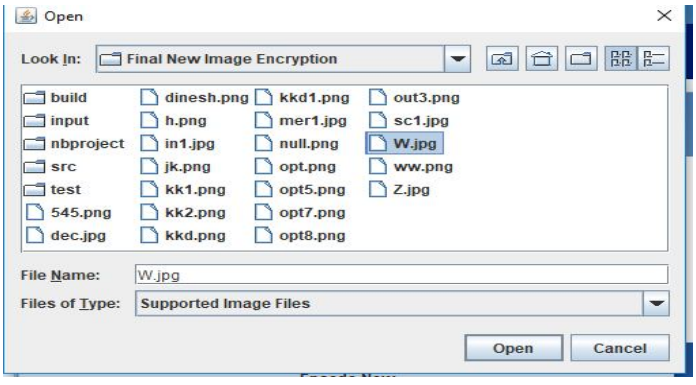
D. Encrypted Image

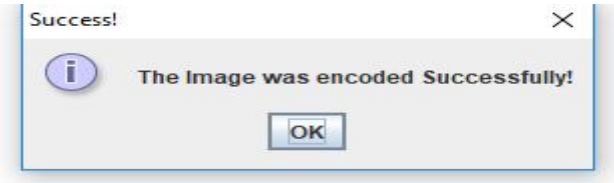


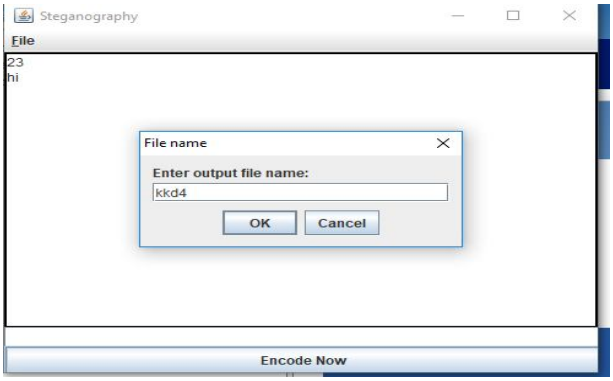
E. Data Hiding Process



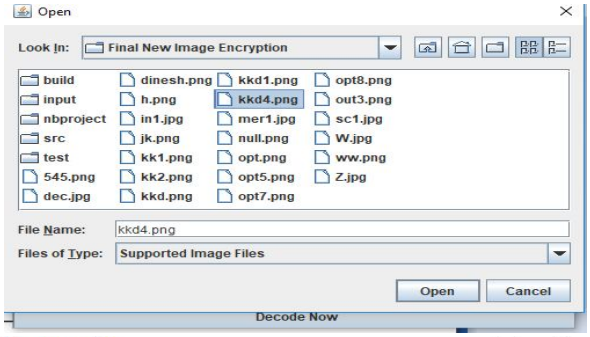
F. Message for Encoding

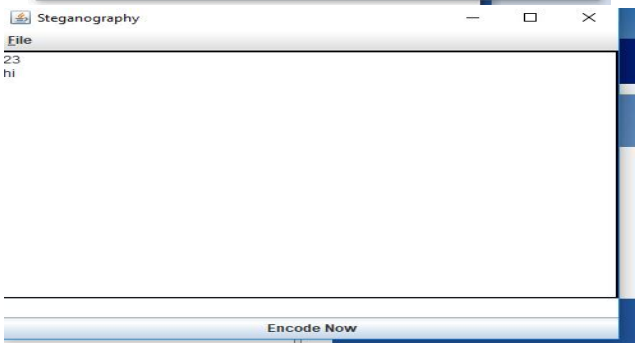


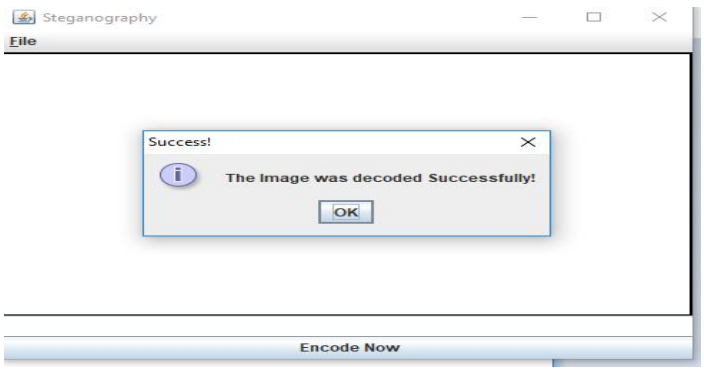




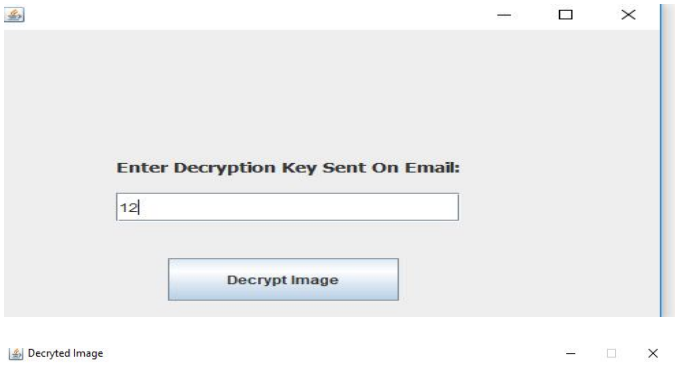
G. Decoding Message







H. Decryption of Image



Decrypted Image

VI. CONCLUSION

This system usage SVD algorithm for encryption and gain better quality of image. The information hider can profit from the data-embedding space reserved by the color dividing procedure, and put on the color changing method to embed the added data. The data separation and image retrieve are separable and freebie of any error.The message which is encoded and decoded accuratly in the image.The further more work will be extending for video making.

REFERENCES

[1] J. Fridrich, M. Goljan and R. Du, “Invertible authentication,” Proc. SPIE, San Jose, CA, vol. 3971, pp. 197-208, 2001.
[2] Jun Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 2003
[3] Z. Ni, N. Ansari and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006.
[4] V. Sachnev, H. Joong Kim, J. Nam, S. Suresh and Y. Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, 2009.
[5] X. Wang, X. Li and B. Yang, “Efficient generalized integer transform for reversible watermarking,” IEEE Signal Process. Lett. vol. 17, no. 6, pp. 567-560, 2010.
[6] C. Li , “A secret-sharing-based method for authentication of grayscale document images via the use of the PNG image with a data repair capability,” IEEE Trans. Image Process., vol. 21, no. 1, pp. 207-218, 2012.
[7] R. A. Sadek, “SVD Baesd Image processing Applications: state of The Art, Contributions and research challenges”, IJACSA, Vol. 3, No. 7, 2012.
[8] X. Li, W. Zhang and X. Gui , “A novel reversible data hiding scheme based on two-dimensional difference-histogram modification,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1091-1100, 2013.
[9] K. Ma, W. Zhang, X. Zhao and N. Yu, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553-562, 2013.
[10] J. Rao, S. Jankar, “Grayscale Image Authentication and Repairing”, IJRET, Volume: 02 Issue: 09, 2013.
[11] J. Rao, S. Jankar, “Image Tampering Detection and Repairing, International Journal of Computer Applications (0975 – 8887) Volume 85 – No 17, 2014.
[12] X. Cao, L. Du, X. Wei, D. Meng and X. Guo, “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” IEEE Trans. Cybernetics, [Online Available], 2015.
[13] Han-Zhou Wu, Yun-Qing Shi, Hong-Xia Wang and Lin-Na Zhou, “Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification.” IEEE Trans. Circuits Syst. Video Technol., 2015.