

# STRING RECOVERY IN AN ENCRYPTED IMAGE USING REVERSIBLE DATA HIDING TECHNIQUE

ANUPAMA<sup>1</sup> & Dr.G.SREENIVASULU<sup>2</sup>

<sup>1</sup>M.TECH STUDENT, DEPT OF ECE, SRI VENKATESWARA UNIVERSITY COLLEGE OF ENGINEERING, TIRUPATI

<sup>2</sup>PROFESSOR, DEPT OF ECE, SRI VENKATESWARA UNIVERSITY COLLEGE OF ENGINEERING, TIRUPATI

Received: June 24 , 2018

Accepted: August 07, 2018

## ABSTRACT

*This brief presents, a reversible data hiding technique for encryption and decryption of images supported the progressiverecovery inconjunction with the string hiding technique. During this technique, three phases are implemented. They are encryptionstring hiding, Decryption. In encryption, a secret image is embedded into the initial image to make an encrypted image. In string hiding technique, a string is hidden among the encrypted image. Finally among the decryption stage, the secret image is decoded from the initial image and thus the string hidden among the encrypted image is in addition decoded with none errors. Whereas most of the conventional ways that use one criterion to recover the whole image, we tend to propose to do and do the recovery by a progressive mechanism. Rate-distortion of the proposed technique outperforms progressive RD H-EI strategies.*

**Keywords:** Reversible data hiding, information hiding, encrypted image

## I. INTRODUCTION

Communication of digital statistics turns into frequent in recent times, because of its brief get right of entry to functionality. A terrific range of Technology for end-to-end protection are required to face up to the security threats. In stylish communication. Data interest and cryptography are the two most important strategies for relaxed Communication. In cryptography, the apparent information is modified into an unreadable type called ciper facts. Modified into an unreadable kind called ciper information. The dilemma of cryptography is that the third party of often conscious about the verbal exchange of incomprehensible statistics. In statistics hiding, the records is hidden in an incredibly cover file and it is going to be transmitted over the community. Activity the lifestyles of secret facts are that the primary advantage of facts hiding techniques over cryptography. Digital watermarking, steganography and reversible facts hiding (RDH) are the sorts of data hiding (RDH) are the types of facts hiding methods. Data hiding will be a way to enter similarly facts into virtual multimedia via to go into similarly information into virtual multimedia with the aid of slightly sterilization the cover signals. Once the statistics hiding is performed with reversible way, the authentic cowl content may be flawlessly restored once information extraction at receiver truth. The reversible records concealment approaches could also be more or less categorized into three approaches: The difference growth methods,

histogram modification approaches, and additionally lossless compression primarily based approaches.

Within the distinction expansion ways, the variations between 2 adjacent pixels are doubled to generate a new pixels are doubled to generate a new least significant bit (LSB) plane for embedding the histogram modification methods shift the histogram of cover data from its peak point towards its zero points, and utilize the cover data at the peak point histogram to carry the additional data hiding, the lossless compression based total ways create use of statistical redundancy of the host media by performing lossless compression in order that a spare space for accommodating the additional data is also created.

As is documented, encoding is an efficient and widespread means that of privacy protection. Therefore, one should not share a secret image with a totally different person, a content owner might encrypt the image before transmission. In some applications, In some applications things, an inferior assistant or a channel administrator hopes to append some further message, corresponding to the origin data, image notation or authentication data, among the encrypted image although he doesn't understand the initial image content. as an instance, once medical image are encrypted for shielding the medical image are encrypted for shielding the patient privacy, {a data|knowledge|an information} administrator might aim to insert the private data into the corresponding encrypted images. It's planning to

be additionally hopeful that the initial content are recovered with none be recovered with none error once cryptography and retrieve of further message at receive aspect. which means a reversible aspect? which means a reversible datahiding theme for encrypted image is fascinating.

This work proposes a completely unique reversible particular reversible data hiding topic for encrypted image it really is created of image encryption, data embedding and records-extraction image -restoration phases. The informationinfacts of original cowl are entirely and additionally the more message is embedded through enhancing enhancing a place of encrypted information. At receiver component, with the assistance of spacial correlation in herbal image, the embedded information are with achievement extracted wherever due to the fact the initial image is absolutely recovered.

**II. EXISTING METHOD**

The existing method of the our method consists of the encryption and decryption of images with generation of the key. The block diagram of the above this existing method is given below:

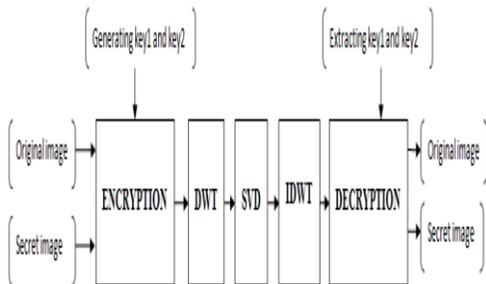


Figure 1: Block diagram of the existing method

**Encryption:**

Encryption could be a method that uses a finite set of instruction referred to as an algorithmic rule to convert original message, calledplaintext, into cipher text, its encrypted kind. Cryptographic algorithm normally needs a set of characters called a key to encrypt decryptdata. Here, the original image and secret image is encrypted based on the key one and key two.

**Discrete Wavelet Transform (DWT):**

In numerical evaluation and practical analysis, a discrete wavelet transform (DWT) is any wavelet transformthat the wavelets are discretely sampled. Like opportunity wavelet transforms, a key benefit it's over Fourier transforms is temporal decision: it captures every frequency and location data (location in time).

During this algorithm HAAR remodel is hired for wavelet remodel.

**Singular Value Decomposition (SVD):**

In algebra, the singular really worth decomposition (SVD) may be a factorization of a true or advanced matrix. It is the generalization of the Eigen decomposition of a high quality semi particular historical matrix (as an example, a radial matrix with positive Eigen values) to any m x n matrix thru an extension of the polar decomposition. It is several useful packages in sign method and information.

Formally, the singular cost decomposition of an m x n actual or complicated matrix M may be a factorization of the shape  $U\varepsilon V^*$ , everywhere U is an m x m real or superior unitary matrix,  $\varepsilon$  is a m x n square diagonal matrix with non-horrible real numbers on the diagonal, partner degreed V is an n x n actual or superior unitary matrix. The diagonal entries  $\sigma_i$  of  $\varepsilon$  are known as singular values of M.

The columns of U and additionally the columns of V are stated because the left-singular vectors and right-singular vectors of M, severally.

The singular cost decomposition may be computed the use of the subsequent observations:

- The left-singular vectors of M are a fixed of orthonormal eigenvectors of  $MM^*$ .
- The right-singular vectors of M are a set of orthonormal eigenvectors of  $M^*M$ .
- The non-0 singular values of M (located on the diagonal entries of  $\Sigma$ ) are the rectangular roots of the nonzero eigen values of each  $M^*M$  and  $MM^*$ .

Applications that use the SVD include computing the pseudo inverse, statistical method becoming of information, multivariable control, matrix approximation, and determinative the rank, variety and null area of a matrix.

**Decryption:**

Decryption is the procedure of extracting the name of the secret image from the original image. For this decryption method, we once more apply the keys on the receiver for the authentic photo and for the secret image to decrypt them.

**III. PROPOSED METHOD**

In our method we encrypt a secret image within the authentic beside a string to be transmitted in secret without any mistakes. This approach moreover passes the hidden string to the receiver moreover as the secret image through generating keys for each the name of the secrete image and the unique image.

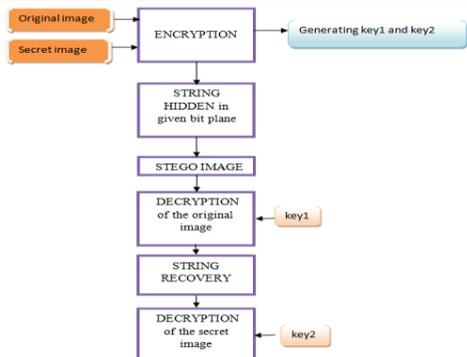


Figure 2: Block diagram of the proposed system

**Original image:**

The original image is that the image of any format that is employed as a cover image to hide each secret image and therefore the string. The key1 is generated for the initial image for safe transmission.

**Secret image:**

The secret image is that the image that's to be embedded within the original image by generating key a pair of to transmit the image safely. Whereas transmission, the initial image is merely visible to the intermediates and therefore the secret image is hidden in it.

**Encryption:**

Encryption could be a process that uses a finite set of instruction referred to as associate degree algorithm to convert original message, called plaintext, into cipher text, its encrypted form. Cryptologic algorithms ordinarily require a collection of characters referred to as a key to encrypt or decrypt data. Here, the original image and secret image is encrypted supported the key one and key a pair of. Algorithm In image encryption process, the given image is converted into the sequence of bytes. Once the bytes are converted to the numeric integer value, it's going to contain positive or negative value as hold on in byte array. Before encryption, the value in byte array has been converted as positive values. These values forms the position of Mr. Finally, the encryption process is being performed using any algorithmic program available in the public key cryptography. Then the resulting cipher text is changed to retain the original sign based on the bytes generated at the initial stage.

**Hiding a string:**

After the cryptography of the secret image and the original image a string that's to be transmit to the receiver without any recovery of the image without using the private key. In this method the entire image is divided into bit planes and we will embed the string in the color

original image in any of the bit plane. Then it calculates the quantity of bytes for the string if that value is beyond the limit of the image size then the string is embedded without any issue. Then finally the string is hidden in the image.

**Decryption of the image:**The decryption is the method of holding the original image at the receiver by giving the private key. If the key is matched then the initial image is decoded beside the string hidden within the cover image. Then the on applying key a pair of the secret image embedded within the original image is decoded. By this approach, the user who is aware of the non-public key will only acquire the encrypted string and therefore the secret image.

**Advantages:**

- **Imperceptibility:** Passing undetected data technique by Human visual system(HVS) is its capability.
- **Security:** To attack even after realization of data can be attained by this.
- **Robustness:** It is the ability of the stego object to oppose unintentional actions like filtering, cropping, rotation, compression, etc.

**Applications:**

- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems

**IV. RESULTS**

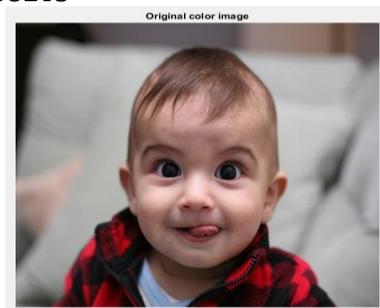


Figure 3: original color image



Figure 4: secret color image



Figure 5: Encrypted image

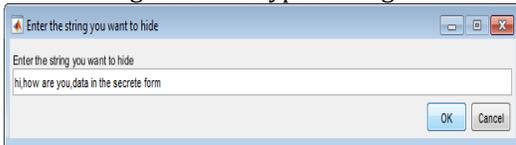


Figure 6: Enter the string you want to hide

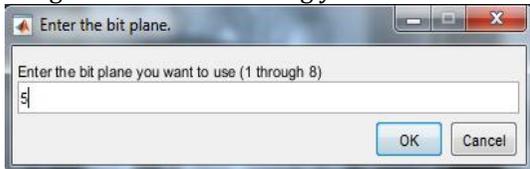


Figure 7: Enter the bit plane to insert the image

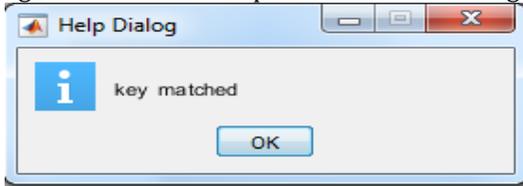


Figure 8: Key matched or not matched dialog box



Figure 9: Help dialog to show recovered string



Figure 10: Retrieved secret image

**PSNR (Peak Signal to Noise ratio):** Calculated usually in logarithmic (dB) scale is a metric use to measure the quality of any image reconstructed, restored or corrupted image with respect to its reference or ground truth image.

$$PSNR = 10 * \log_{10}(256 * 256 / MSE)$$

$$MSE = \frac{\sum(\sum(Input - output)^2)}{(M * N)}$$

**MAE:** Mean absolute error (MAE) is a measure of difference between two continuous variables.

$$MAE = \frac{\sum_{i=1}^n |y_i - x_i|}{n} = \frac{\sum_{i=1}^n |e_i|}{n}$$

Parameters	Existing system	Proposed system
MAE	28.67	14.39
PSNR	8.25	16.33

## V. CONCLUSION

In this paper a reversible data hiding technique is enforced by using progressive recovery along with a secret image is additionally embedded in it. During this approach, encryption, string hiding, decryption of the images along with the string hidden is performed. In secret writing, a secret image is embedded into the initial image to make an encrypted image. In string hiding method, a string is hidden inside the encrypted image. Finally in the decryption stage, the secret image is decoded from the preliminary image and therefore the string hidden in the encrypted image is moreover decoded without any errors. Our proposed method to attempt to do the recuperation by a innovative method will provide higher outcomes compared to the state off art ways. Rate-distortion of the proposed approach outperforms progressive RDH-EI approaches.

## REFERENCES:

1. X. Hu, W. Zhang, X. Li, and N. Yu, Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding, IEEE Transactions on Information Forensics and Security, 10(3): 653-664, 2015.
2. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253-266, Feb. 2005.
3. X. Zhang, Reversible data hiding in encrypted snap shots, IEEE Signal Processing Letters, 18(4): 255-258, 2011 [6] W. Hong, T. Chen, and H. Wu, An stepped forward reversible statistics hiding in encrypted pix the usage of component in shape, IEEE Signal Processing Letters, 19(4): 199-202, 2012.
4. S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774-778, 2007.
5. Z. Qian, X. Zhang, and S. Wang, Reversible records hiding in encrypted JPEG bit glide, IEEE Transactions on Multimedia, 16(five): 1486-1491, 2014.