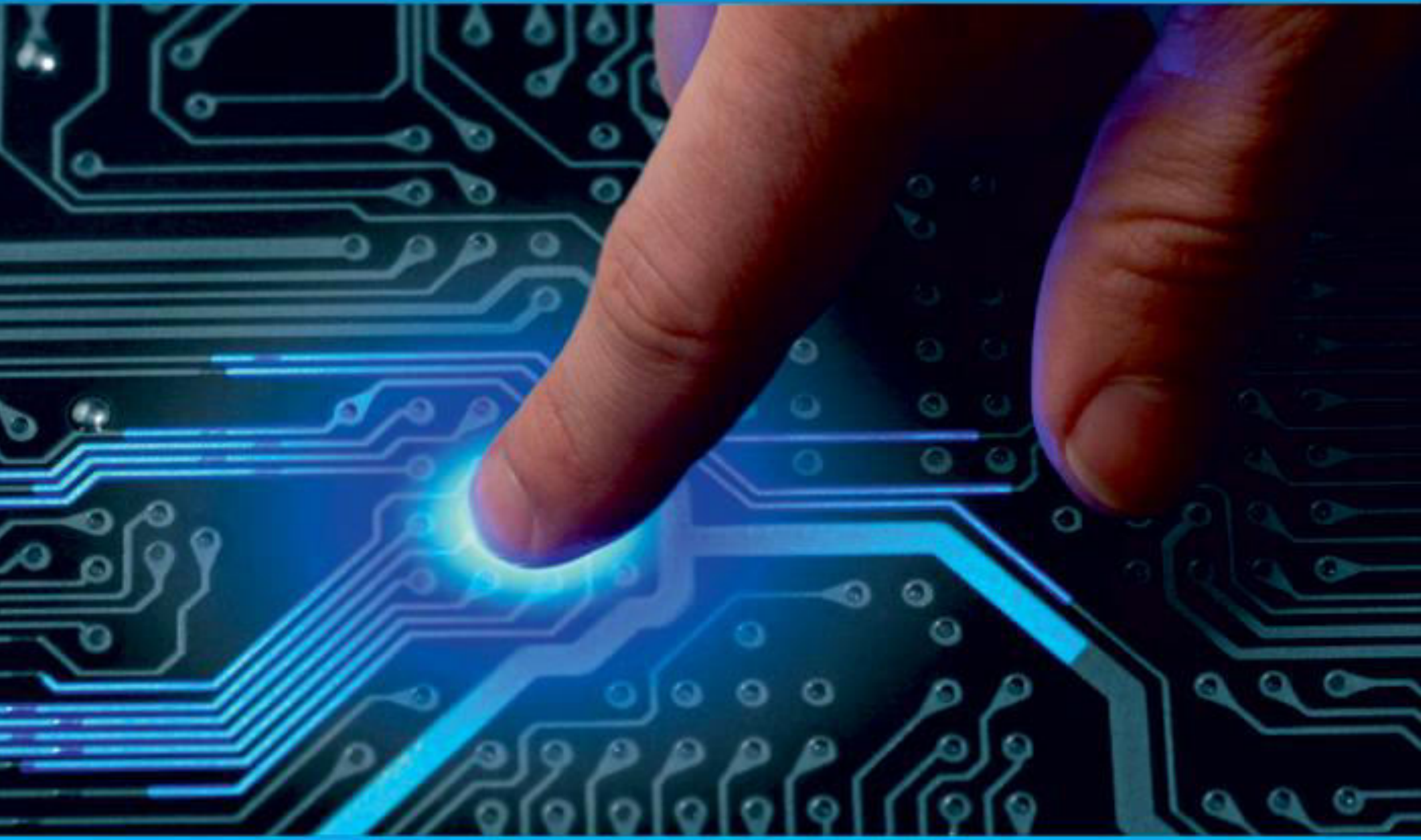
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102028 |

Reversible Data Hiding In Encrypted Images

Poonam Koli[1], Rasika Ladage[2], Poonam Bavache[3]

Lecturer, Dept. of ENTC., DKTE YCP, Ichalkaranji, Maharashtra, India

ABSTRACT: This paper proposes reversible data hiding in encrypted images for secure missile launching. The work is presented in two stages: one involves encryption of cover image by block cipher algorithm and other is embedding secure data related to missile launching. For embedding data, vacant pixels are identified by Slepian-Wolf encoding method along with embedding key to hide the data. At the other end by using decryption algorithm the original cover image is recovered and the secret data is extracted. The performance analysis is presented by calculating parameters MSE, PSNR and SSIM.

KEYWORDS: Image Encryption, Data Embedding, Reversible Data Hiding.

I. INTRODUCTION

In many applications, like law forensics, military imagery and medical imagery the information vendor requires to transmit data to a distant server for future processing. Now a day, internet is the prime medium to transfer information from one end to another across the world. The additional secret information can be hacked in a lot of different ways. This is the major problem with sending information over the internet. Therefore it becomes very important to take data security into consideration, during the procedure of data transferring. The intruder may also capture image, and view the significant contents and then alter the image before transferring it to receiver [1]. This is the way by which original image contents will be modified and receiver cannot have an idea about it. In general, a bit of content distortion is typically imperceptible to human imaginative. However, such distortion is not favored in some applications, like legitimate documentation, medical imaging, military observations, high-accuracy scientific investigation, since it might prompt risk of wrong decision making. Data security basically means given that safety to information from unauthorized users or hackers and imparting excessive level of protection to prevent information from modification. Data hiding is one kind of approach to secure data in cover media but there exists some distortion. In data hiding method the private and secret information is hidden into cover (host) image.

II. PROPOSED METHODOLOGY

The general structure of the proposed method is presented in Figure 1, which consists of 4 phases, namely image encryption, data hiding, image recovery, data extraction, and the last unit of missile launching.

The original cover image is first transformed into encrypted image using encryption algorithm. The data hider embeds the additional secret information into encrypted image using an embedding key to generate embedded image.

At the receiving end, receiver extracts the inserted secret information independently only if it has an embedding key. If receiver has knowledge about encryption algorithm and embedding key both, the inserted secret bits can be extracted and original cover image can be recovered.

Image Encryption

Original image must be grayscale; if input image is color then we first convert it into grayscale (0 to 255). The image is preprocessed such as image resizing and converted into particular intensity range. The mathematical operations on the image may results into negative value or may exceed the upper boundary. At recovery stage this may result in receiving the random symbols like $, #, etc. To avoid such circumstance at receiving end we set intensity range of image to 15 and 240.

Encryption is not directly applied on whole image; we select non-overlapping blocks from cover image. We divided selected block into two sub regions and then calculate pixel difference value and integrative component. Again we further divided the result obtained into two sub regions resulting into total four sub regions. For these four sub regions we calculated the difference and integrative components labelled as c1, c2, c3, and c4. We shuffled all the four This decomposition and combing process is applied for each and every non overlapping block of cover image. Combined results (c2, c1, c4, c3) of each block, result into total encrypted image. components before combining them. We have not used any shuffling key, shuffling is done by simply rearranging the four components in different order (like c2, c1, c4, c3).

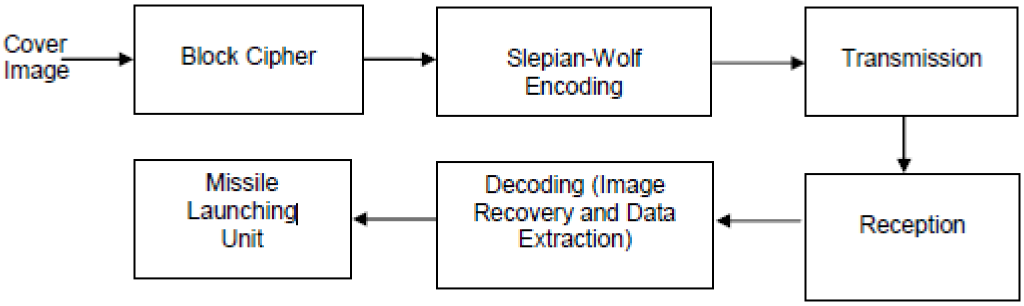


Fig 1: Proposed System

Data Hiding

The Slepian-Wolf encoding method is used for data hiding. To compress the selected bits from encrypted image the Slepian-Wolf codes are useful. Defined low density parity check code (LDPC) matrix **H,** it can be constructed in various different forms. The data-hider arbitrarily chooses a parity-check matrix **H** corresponding to a regular or irregular LDPC code by setting the numbers of variable nodes and the check nodes. The different algorithms have been proposed for the matrix construction, for example, matrices used in Gallager codes, MacKey codes, and finite geometry codes. For example by using MacKey method the matrix is constructed by following steps

1. The H matrix is created by initially creating all zero matrix and then randomly flipping bits in the matrix H. The flipped bits must not be necessarily distinct.
2. The matrix H is generated by randomly creating weight j columns.
3. The matrix H is generated with weight j per columns and uniform weigh per row and no two columns are connected to the same row more than ones (avoiding four cycles)
4. Matrix H is generated as in step 3 with the girth condition further constrained so that the girth is larger than six.

The MacKey's algorithms were used to find good performing codes with the variety of length and rates. The more details of LDPC matrix **H** can be found in [14].

We have selected a non-overlapping blocks of encrypted image for data embedding. We have selected an embedding key and checked for embedding key bit equals to one. And where the embedding key bit is one the value at that position in the selected block of encrypted image is considered as coefficient. We performed matrix multiplication between selected coefficient and H matrix, and the spare room is generated for data embedding. In the vacated room the data is embedded and checked for if we have completed with all secret data to be embedded. Otherwise data embedding process is continued. Along with this we have checked for one more condition, whether we completed with selected block of encrypted image, if done then next block is selected. Finally all non overlapping blocks are combined to form an embedded image which is encrypted image containing secret data. Generated embedded image is transmitted.

Image Decryption

At the receiver side, using the received embedded image, the original cover image can be recovered by decryption algorithm. First we divided the received embedded image into blocks and those blocks are decomposed into four sub regions and applied decryption algorithm on it. We performed exact reverse of the process applied at the transmission side. We have calculated the pixel differences and integrative components for all four sub regions. We combined the obtained results into two sub regions. Again by using these two sub regions we have calculated pixel difference and integrative component and combined obtained results into single block. The process was repeated for each block and all resulted blocks were combined to form decrypted/recovered image.

Data Extraction

In data extraction, we select a non overlapping block of embedded image. We used an embedding key to extracts the embedded secret data. We checked for embedding key bit, if it is one it means data is embedded at that position in selected block of embedded image. The value at that position is considered as coefficient and LDPC matrix is applied on it. From this we get to know the position where data is embedded and those bits are extracted.

Missile Launching Unit

The decrypted secret data are the coordinates required for missile launching. The launching of missile involves coordinates corresponding to azimuth and elevation angle made by missile. Accordingly during embedding process we embedded these coordinates. For example xy120150; where x y is used as an identifier which shows the start of valid bit frame, the next three digits corresponds to azimuth angle and last three digits corresponds to elevation angle. By using the serial communication the extracted data is send to missile launching hardware unit. The hardware unit consists of two DC motors, motor driver circuitry and controller. If identifier is received properly then the received data is treated as the valid frame and the DC motor rotation is made accordingly. The missile is then positioned at the target location. If received identifier does not match then it indicated invalid data received.

III. CONCLUSION AND FUTURE WORK

Here we propose a technique of reversible data hiding in encrypted images and its application to secure missile launching. Initially encryption is applied on original image. Depending upon embedding key, bits of encrypted image are selected and Slepian-Wolf encoding is applied to make spare room for the secret data. At the receiver end, all hidden secret data is extracted using embedding key, also original image is approximately recovered with good quality with the help of decryption algorithm. To generate corresponding syndromes LDPC parity-check matrix is used. On encrypted image we performed data embedding operation, so the data-hider cannot access the contents of the original image. That ensures security of the contents in data hiding. As the embedding and recovery is protected by the encryption and embedding keys, an adversary is unable to break into the system without these keys. The future direction is to improve system performance parameters by considering noisy channel.

REFERENCES

[1] Shilpy Mukherjee, A. Mahajan, "*Review on Algorithms and Techniques of Reversible Data Hiding*" International Journal of Research in Computer and Communication Technology, Vol 3, Issue 3, March- 2014

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

[3] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp and Eli Saber, "*Reversible DATA Hiding*" IEEE ICIP pp. 157-160. 2002.

[4] J. Tian, "*Reversible data embedding using a difference expansion*," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[6] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[7] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[8] ZhenxingQian, and Xinpeng Zhang, "*Reversible data hiding in encrypted images with distributed source encoding*," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 4,pp. 636-646 April 2016.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING