International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 949-952 www.ijaem.net ISSN: 2395-5252

A Novel Approach for Cover Lossless Robust Image Watermarking Against Geometric Deformation

Prof.R.Arunapriya M.E.,(Ph.D).,[1] Assistant Professor, K.Uma,[2] D.Saranya,[3] G.Theerthi,[4] S.Savitha[5]
Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur.

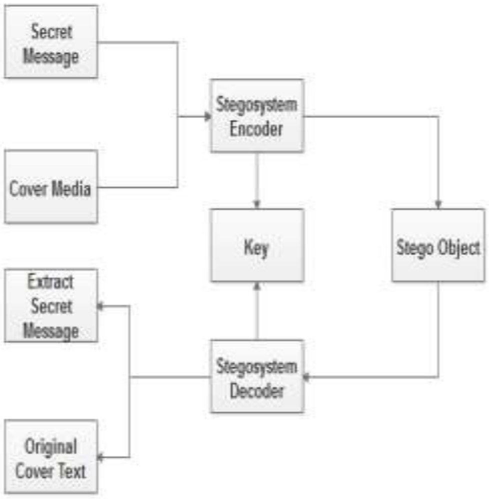
Submitted: 05-05-2021 Revised: 17-05-2021 Accepted: 20-05-2021

ABSTRACT: As an effective means of copyright protection, the digital watermarking technology has attracted wide attention. Traditional digital watermarking can cause some distortion of the original image after embedding some information. But in some special applications, it is required to restore the original image; thus, the reversible digital watermarking emerges as the times require. Different from traditional digital watermarking method, reversible watermarking technology can recover the original host information without distortion after extracting the watermark information, which is badly needed in the area of military intelligence, medical records, and legal argumentation demanding, so it has been widely developed in recent years.

The amplitude of the exploited low-order Zernike moments are: 1) mathematically invariant to scaling the size of an image and rotation with any angle; and 2) robust to interpolation errors during geometric transformations, and those common image processing operations. To reduce the compensation information, the robust watermarking process is elaborately and luminously designed by using the quantized error, the watermarked error and the rounded error to represent the difference between the original and the robust watermarked image. As a result, a cover-lossless robust watermarking system against geometric deformations is achieved with good performance.

I. INTRODUCTION

Modern steganography was characterized by G J Simmons when he stated the problem in terms of prisoners attempting to communicate covertly in the presence of a warden. Alice and Bob, prisoners, are allowed to communicate, but their channel is through the warden, Ward. Alice wishes to pass secret messages to Bob in such a way that Ward can determine neither the contents of the secret messages, nor even that secret messages are being passed. In modern times, this problem can be observed in national intelligence agencies attempting to detect public yet covert communication between terrorists, or communication between citizens in oppressive states which have outlawed cryptography.



II. LITERATURE SURVEY

2.1 Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au and Yuan Yan Tang," Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation"

They proposed an encrypted-domain RIDH scheme by specifically taking the above-mentioned design preferences into consideration. The proposed technique embeds message through a public key modulation mechanism and performs data extraction by exploiting the statistical distinguishability of encrypted and non encrypted image blocks. Since the decoding of the message bits and the original image is tied together, our proposed technique belongs to the category of nonseparable RIDH solutions. Compared with the state-of-theart methods, the proposed approach provides higher embedding capacity and is able to achieve perfect reconstruction of the original image as well as the embedded message bits. Compared with the original unencrypted block, the pixels in the encrypted block tend to have a much more

uniform distribution. This motivates us to introduce the local entropy into the feature vector to capture such distinctive characteristics. If not otherwise specified, the widely used stream cipher AES in the CTR mode (AES-CTR) is assumed. The resulting data hiding paradigm over encrypted domain could be more practically useful because of two reasons.
Merits: Enabling us to jointly decode the embedded message and the original image signal perfectly.
Demerits: The embedding capacity of this type of method is rather limited.

2.2 Monika Bartwal, Dr. Rajendra Bharti,"Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography"

In an image by using the redundancy used a key of reversible data embedding for finding an embedding area. To enlarge the other space the current techniques decrease the redundancy by the execution of pixel value calculation and make use of image histogram. The modern techniques show unlimited embedding volume without severely demeaning the visual excellence of embedded consequence. The first step is image division, the innovative uncompressed image is separated into two fragments A and B; and monitored through the LSBs. A is reversibly embedded into B, using self-reversible inserting and reversible data hiding technique. LSBs of A can be used to put up extra data. Afterward self embedded data reorganized the encodes image using stream cipher. The values are 0 to 255 and signified by 8 bits. Afterward the encryption process, the data hider put up the encoded image, and insert a limited data into it. The data hider can´t change the original image and only can manage the access to the embedded data. The data mining and data extraction entirely differs from image decryption. Two different case are taking to show.

Merits: It produces individually advanced embedded quality of images provided with a same embedding capacity.
Demerits: In This Paper proposed technique cannot be verified on various attacks.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

RHD-EI allows a server to embed additional message into an encrypted image uploaded by the content owner, and guarantees that the original content can be losslessly recovered after decryption on the recipient side. This method strictly relies on the properties of secret sharing. Summarizing the main techniques, secret sharing serves as the underlying primitive offering security, multiple secret preserves size complexity, and inherently additive homomorphism realizes the data embedding. Here provide the formal description of the technique, and present a clear notion, so-called operating addition homomorphism in multi-secret sharing (OAMSS). Also provide another technique to compress the size of a key used in OAMSS. For generalization, if SNK (Share No Secret Key) schemes satisfy some properties, they can be converted to SOK (Share One Key). Hence, this method can be generalized as a converter. As a concrete instantiation, SNK scheme based on difference expansion, we show the SOK-type RDHEI by slight modification.

The scheme overview is described as follows. P will pre-process the coverimage and generate a new cover-image, referred to as the processed image, and then send H the encrypted image by using polynomial interpolation. H will obtain a new polynomial which carries a secret message in the released LSB plane, and then use addition homomorphism to generate the encrypted image with embedded message. Finally, by decryption R is able to obtain the stegoimage, and then recover the cover-image and secret message.
Here provide the formal description of the technique, and present a clear notion, so-called operating addition homomorphism in multi-secret sharing Hence, this method can be generalized as a converter.

Disadvantages

1. Generalization of single secret to that of multiple secrets is a major threat by decrypting a single secret can easily end up with decrypting the remaining shares.
2. (k , n) is also an issue which helps the intruder to decrypt the images when received k or more number of shares.
3. Creating meaningless shares initiates the intruder to try and decrypt the shares.

3.2 PROPOSED SYSTEM

The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This method eliminates the fundamental security challenges of VC like external use of code book, random share patterns, expansion of pixels in shared and recovered images, lossy recovery of secret images and limitation on number of shares.

The proposed method is n out of n multi secret sharing scheme.

Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret text can be hidden within the image in QR format. Teat message was created by sender and converted into QR code format. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. The text is typed and hidden in an image. This is done using LSB method. Then the XOR based VC method is used to encrypt the image and send it to the receiver. The key which is used to encrypt the shares will be mailed to the receiver. The receiver will decrypt the shares using the same key that is used for encryption. After that, the hidden text will be extracted from the recovered image using the LSB method.

Advantages

- The secret image and the recovered image will be of the same size.
- (n , n) technique helps to decrypt only when all the shares are received.
- Multi secret sharing is used to send multiple shares at the same time.

IV. SYSTEM IMPLEMENTATION

MODULE DESCRIPTIONS

1. Text Hidden within QR code

Text hiding is a process of embedding the secret text imperceptibly into the cover media by minimally modifying the elements of the cover media. In this module sender will generate the content for transmit to the receiver. Message text is present in the form of normal text in English words. Uploaded texts message was converted into QR format.

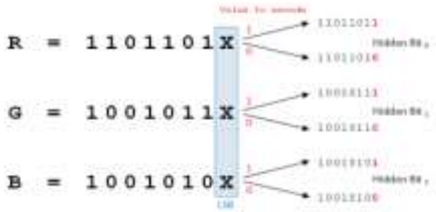
2. Image Upload and Hiding

This process is to select cover media for information hiding. Here images are used as a cover media for the secret message. Cover image is also select by the sender when create the secret message. Original message is hidden into the cover media (image) to improve the security of data sharing. The steganographed image that has to sent should be uploaded. The image should be any one of the image supporting formats. The various supporting formats are JPEG, PNG & BMP. A text is written and hidden inside a secret image. This is done by using LSB method. The cover image is called as a steganographed image.

3. MPVD with LSB Algorithm

In the embedding process of a secret message, a cover image is partitioned into non-overlapping blocks of nine consecutive pixels. A difference value is calculated from these values of the nine pixels in each block. All possible difference values are classified into a number of ranges. The calculated difference value then replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value.

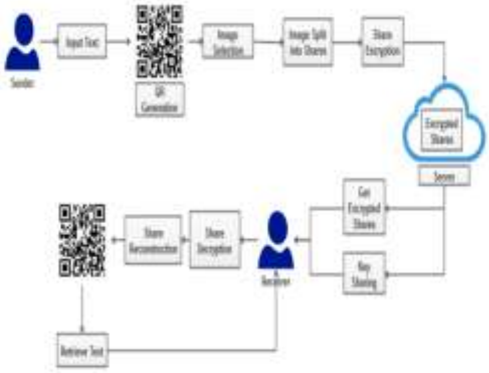
The way of embedding the secret information within the cover file is called LSB insertion. In proposed technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit color images are used to perform LSB, then the amount of modification will be small.



V. SYSTEM DESIGN

SYSTEM ARCHITECTURE

System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability.



VI. SOFTWARE DESCRIPTION

JSP Framework

Java Server Page (JSP) is a technology for controlling the content or appearance of Web pages through the use of servlets, small programs that are specified in the Web page and run on the Web server to modify the Web page before it is sent to the user who requested it. Sun Microsystems, the developer of Java, also refers to the JSP technology as the Servlet application program interface (API). JSP is comparable to Microsoft's Active Server Page (ASP) technology. Whereas a Java Server Page calls a Java program that is executed by the Web server, an Active Server Page contains a script that is interpreted by a script interpreter (such as VBScript or JScript) before the page is sent to the user. Architecturally, JSP may be viewed as a high-level abstraction of Java servlets. JSPs are translated into servlets at runtime, therefore JSP is a Servlet; each JSP servlet is cached and re-used until the original JSP is modified.

VII. SYSTEM TESTING

TESTING PROCESS

Software testing is a method of assessing the functionality of a software program. There are many different types of software testing but the two main categories are dynamic testing and static testing. Dynamic testing is an assessment that is conducted while the program is executed; static testing, on the other hand, is an examination of the program's code and associated documentation. Dynamic and static methods are often used together. Testing is a set activity that can be planned and conducted systematically. Testing begins at the module level and work towards the integration of entire computers based system. Nothing is complete without testing, as it is vital success of the system.

Testing Objectives:

There are several rules that can serve as testing objectives, they are;

1. Testing is a process of executing a program with the intent of finding an error
2. A good test case is one that has high probability of finding an undiscovered error.
3. A successful test is one that uncovers an undiscovered error.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. In this work, a text message was hidden within QR Code then the QR will be hidden within image. The sender has to create text and generate QR for input text then select the image to hide the QR image using MPVD with LSB approach that should be sent the message secretly to the receiver. Then the secret image is splitted into "n" number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image. Multi secret sharing is used to send multiple shares at the same time.

FUTURE ENHANCEMENT

Authentication has to further improve in future. Also the noise level should be decreased during image split and merge. This is considered as the future work of the proposed project.

REFERENCES

[1]. Bartwal, Monika, and Rajendra Bharti. "Lossless and Reversible Data Hiding in Encrypted Images With Public Key Cryptography." Annals of Computer Science and Information Systems 10 (2017): 127-134.

[2]. Cao, Xiaochun, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo. "High capacity reversible data hiding in encrypted images by patch-level sparse representation." IEEE transactions on cybernetics 46, no. 5 (2015): 1132-1143.

[3]. Chuman, Tatsuya, Kenta Iida, and Hitoshi Kiya. "Image manipulation on social media for encryption-then-compression systems." In 2017 AsiaPacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 858-863. IEEE, 2017.

[4]. Chuman, Tatsuya, Kenta Kurihara, and Hitoshi Kiya. "On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks." IEICE TRANSACTIONS on Information and Systems 101, no. 1 (2018): 37-44.

[5]. Dragoi, Ioan Catalin, Henri-George Coanda, and Dinu Coltuc. "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction." In 2017 25th European Signal Processing Conference (EUSIPCO), pp. 2186-2190. IEEE, 2017.