IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 7, May 2023

Reversible Data Hiding in Images by MSB Prediction

Raut Ayush Dinesh, Pathan Sohel Tayyab, Khatik Khalid Jakir,
Pawar Satyajeet Madhav, Prof. Varsha Goosavi
Smt. Kashibai Navale College of Engineering, Pune, India

Abstract: Transmission of secret remote sensing or military photos has become more difficult due to the advancement of new media technology. Studying the technique for securing these secret photographs is a new and difficult endeavour. In this paper, a novel two-channel deep hiding network (TDHN) is designed based on the powerful spatial feature extraction capability of the convolutional neural network by introducing advanced ideas such as skip connection, feature fusion, and so on, and the two channels are used to simultaneously input the cover image and the secret image. There are two sections to this network: the concealment network and the extraction network. The sender employs the hiding network to conceal a secret image within a standard cover image, resulting in a hybrid image known as the hidden image. To extract and recreate the secret image from the hidden image, the receiver employs the extraction network. Meanwhile, two measures called MSE and SSIM are used to create a novel loss function. The TDHN optimised by the loss function may generate a high-quality concealed image and extracted image, according to the results. Between the concealed picture and the original cover image, the SSIM value is around 0.99, and between the extracted image and the original secret image, it's around 0.98. It has been proven through testing on various datasets that the developed and optimized TDHN has great generalisation potential, and so has significant theoretical and engineering utility.

Keywords: partitioning algorithm, error correction capacity, high security, Quick Response code, visual secret sharing scheme

I. INTRODUCTION

Many developments have been made in the field of digital media over the last decade, and there has been a lot of anxiety about steganography for digital media. Steganography is a unique way of information concealment. It embeds messages into a host medium in order to hide secret messages from eavesdroppers. A typical steganographic application involves covert communications between two parties whose existence is unknown to a potential attacker and whose success is contingent on detecting their existence. In general, relevant digital media such as digital images, text, audio, video, and 3D models are employed as the host medium in steganography. With the growing popularity and use of digital photographs, a great number of image steganographic algorithms have been investigated.In the field of remote sensing, there is currently little demand for accurate localisation. Detection rather than localisation is the focus of the vast majority of research (the two processes have been confused by some people). Detecting objects in remote sensing photos is significantly more difficult than in natural images due to the more complicated background information they carry. Remote sensing photographs provide information about the texture, shape, and structure of things on the ground, and they can be used to identify them precisely. They do, however, create information redundancy issues in addition to giving adequate information for object detection. Object detection in remote sensing photographs is also a difficult problem due to noise interference, weather, illumination intensity, and other factors.

1.1 Organization of Paper

The organization of the paper is as follows section II gives the related work and limitations and last section concludes the paper with future work followed by references.

DOI: 10.48175/IJARSCT-10187

II. RELATED WORK

The paper [1] proves that the contrast of XVCS is $\mathbf{2^{(k-1)}}$ times greater than OVCS. The monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.

This paper [2] propose sharing QR code secrets explodes the error correction mechanism inherent in the structure of the QR code, for distribute and encode information about a secret message into a number of actions. Each action in the scheme is constructed from a QR cover code, and each share itself is a valid QR code that can be scanned and decoded by a QR code reader. Advantages are: The secret message can be recovered the secret message can be recoveredby combining the information contained in the QR code shares. Disadvantages is: secrete sharing depends on code words.

This paper [3] propose Naor and Shamir has numerous applications, including visual authentication and identification, steganography, and image encryption and introduce cryptanalyze the CPVSS scheme and show that it is not cheating immune. They also outlinean improvement that helps to overcome the problem.Advantage is introduce advance cheating-prevention visual secret-sharing. Disadvantages is prevention accuracy is low.

In [4] paper, present a blind, key based watermarking technique, which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses a unique image code for the detection of image distortion. The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker. Advantages are: More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks. Disadvantages are: Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial domain is more susceptible to attacks this cannot be used.

Visual cryptography [5]i.e. multiple image visual cryptography (MIVC), optimal grayscale reserving visual cryptography (GRVCS) are studied. Embedded extended visual cryptography scheme (Embedded EVCS), simulated-annealing-based algorithm to use the VC construction problem to find the column vectors for the optimal VC construction, natural-image-based VSS scheme (NVSS scheme).

In [6] paper, design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.

The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication [7]. The public level is the same as the standard QR code storage level; therefore it is readable by any classical QR code application. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using QR code with an error correction capacity. Advantages are: It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.

To protect the sensitive data, [8] paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. Advantages are: The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. Only the authorized user with the private key can further reveal the concealed secret successfully. Disadvantages are: Need to increase the security.

In this work [9], HVC construction methods based on error diffusion are proposed. The secret image is concurrently embedded into binary valued shares while these shares are half toned by error diffusion—the workhorse standard of half toning algorithms. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images.

DOI: 10.48175/IJARSCT-10187

This paper [10] author implement an improved algorithm. To start with, the carrier image uses contourlet change to separate the low-frequency part of the image. And it is partitioned into blocks. In addition to the position patterns and separator symbol image, the QR code as watermark information is scrambled transformation. At that point every one of the QR code data to measure the watermark is inserted into each block low-frequency image.Disadvantgaes are: This system basically worked on scrambling transformation and only focus on copy write protection.

In this paper [11], the schemes of user-friendly visual secret sharing dependent on random grids are compared to a proposed scheme. The outcomes show that the proposed schema other than not requiring the Codebook, is more adaptable in the quality control than some different schemas and proposed strategy is that separated from the utilization of complementary cover images, different cover images can be utilized and shares do not contain any follow from one another, which it expands the security and more confusion against attackers.

In this paper [12], as first part, many types of secret sharing schemes are examined and author proposed two Variant of a secret sharing scheme using Gray code and XOR operation. The Gray code is used to construct the shares and the XOR operation is used to reconstruct the secret. The proposed method can be used as a cryptographic algorithm and also for secret sharing as well as visual secret sharing.Disadvatages are: in this paper worked on cryptographic algorithm for data security. Security is less.

In this paper [13], author proposed visual secret sharing scheme using Boolean and shift operations that provides high security to the secret image is designed. An algorithm is proposed to encode the original secret image to generate n share images using simple Boolean XOR and circular shift operations. The secret data cannot be revealed with any $k-1$ or less number of share images. The security is provided to the original secret by encrypting this secret with a random image and distinct authentication id used for each share during generation of shares. The size of generated share images is same as that of original image and requires no pixel expansion. Disadvantage is: This paper used construct two variant secret sharing schemes depend on gray scale images.

In this paper [14], author proposed visual secret sharing scheme share two color images on rectangular shares with no pixel expansion. The originality of secret is verified by watermark which is embedded into the secret image followed by the sharing process. The secret is reconstructed and watermarks are retrieved from the original secret to perform authenticity. Disadvantage is: In this paper worked on DWT and DCT techniques. Security is less in watermarking.

III. PROPOSED METHODOLOGY

In proposed system, a novel approach is introduced to improve the security of QR codes using advanced partitioning algorithm. An existing sharing technique is subjected to loss of security. On this premise, consider the strategy for (k, n) get to structures by using the (k, k) sharing occurrence on each k-member subset dependent on specific relationship. This methodology will require countless examples as n increments. Therefore, presents partioning calculations to group all the k-member subsets into a few assortments, in which cases of various subsets can be supplanted by just one. The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of visual sharing schema. Only the authorized user with the private key can additionally uncover the covered mystery effectively.

Advantages of proposed system

- Efficient and Secure embedding of text.
- Increases security using advanced partitioning algorithm.
- Increases the sharing efficiency.
- Increasingly adaptable access structures and high security.
- Processing cost is less.
- Message accuracy can be checked with hashing technique.

Architecture

Following fig.1 shows the proposed architecture of the given approach:

DOI: 10.48175/IJARSCT-10187

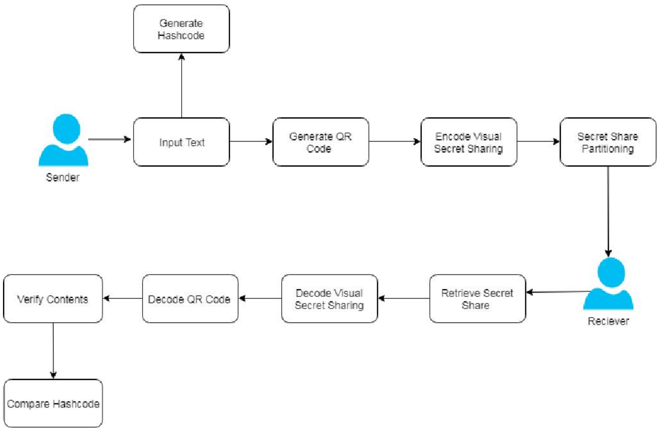


Fig. 1. Proposed System Architecture

Algorithms

Encoding

Representation of each letter in secret message by its equivalent ASCII code.

- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts. Picking of random letters relating to the 4 bit parts.
- Meaningful sentence development by utilizing letters got as the main letters of reasonable words.
- Omission of articles, pronoun, relational word, intensifier, was/were, is/am/are, has/have/had, will/will, and would/ought to in coding procedure to give adaptability in sentence development.
- Encoding isn't case touchy.

Decoding

Steps:

- First letter in each word of encoded message is taken and represented by 4 bit number.
- 4 bit binary numbers of merged to obtain 8 bit number.
- Finally encoded message is recovered from ASCII codes.

IV. MATHEMATICAL MODEL

Let us consider S as a system for Data Hiding System.

S=

INPUT:

Identify the inputs

F= f1, f2, f3 ....., FN— F as set of functions to execute commands.

I= i1, i2, i3—I sets of inputs to the function set

O= o1, o2, o3.—O Set of outputs from the function sets,

S= I, F, O

I = Image, Text

O = Output i.e. Message security

F = Functions implemented to get the output

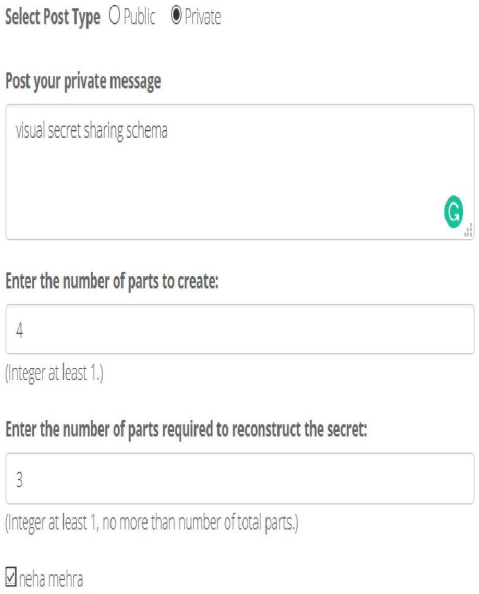
V. RESULTS AND DISCUSSION

Experiments can be performed on a personal computer with a configuration: Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB memory, Windows, MySQL backend database and Jdk 1.9. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

DOI: 10.48175/IJARSCT-10187
ISSN 2581-9429 IJARSCT

The QR code security with texture patterns by applying the X-ORing based Visual Cryptography Scheme on QR code for sharing secrets to the receiver. The figure shows the QR code example. The experiment includes two processes encryption process and decryption process.

Sender:
Enter message, number of parts to create, enter the number of parts required to reconstruct the secret and specific user participants.



Select Post Type ○ Public ● Private

Post your private message

visual secret sharing schema

Enter the number of parts to create:

4

(Integer at least 1.)

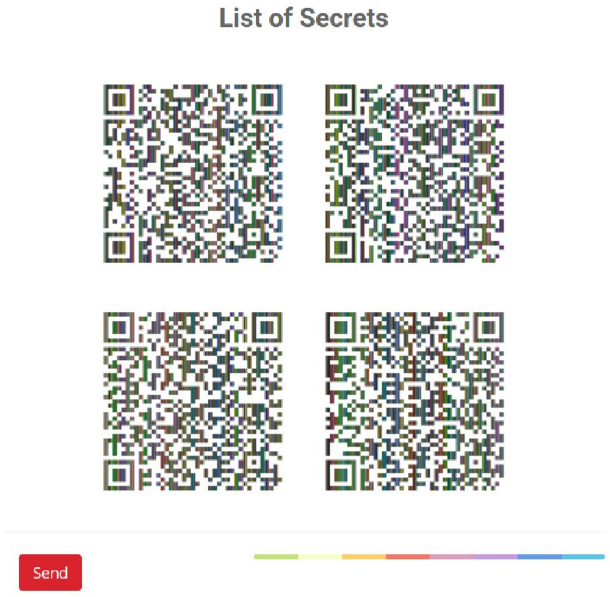
Enter the number of parts required to reconstruct the secret:

3

(Integer at least 1, no more than number of total parts.)

☑ neha mehra

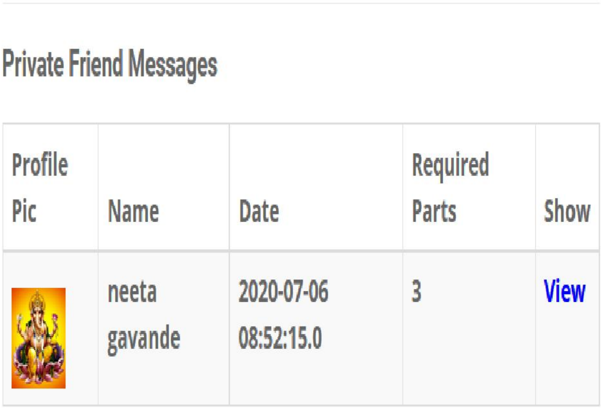
Message – visual secret sharing schema
Generated Hash code of message - 3750f73ed81827d4e6934c09231cbc2c.
Generate number of Parts using advanced partitioning technique i.e. k-means clustering



List of Secrets

Receiver:

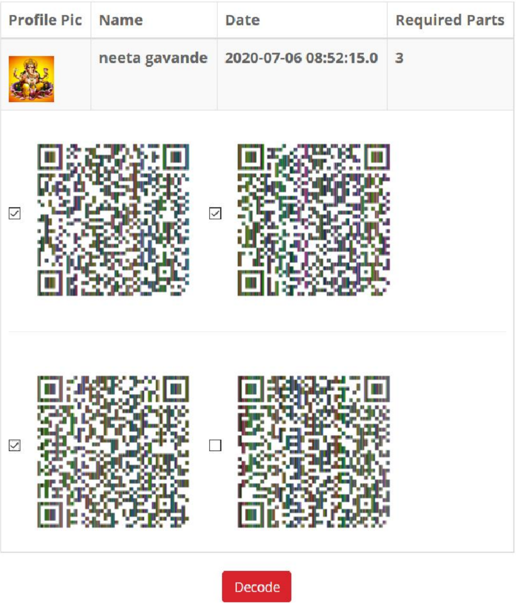
View Message:



Private Friend Messages

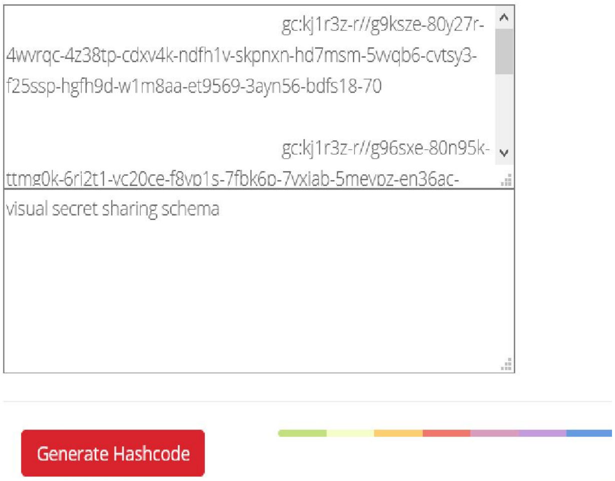
Profile Pic	Name	Date	Required Parts	Show
	neeta gavande	2020-07-06 08:52:15.0	3	View

Select required parts:



Profile Pic	Name	Date	Required Parts
	neeta gavande	2020-07-06 08:52:15.0	3

Decode Message:



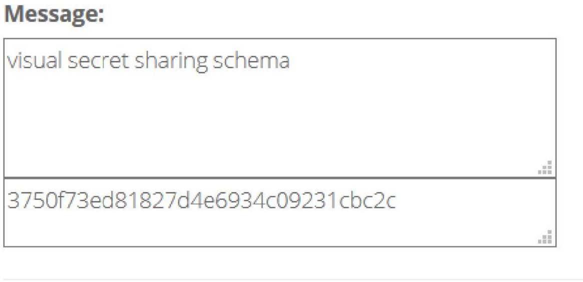
gc:kj1r3z-r//g9ksze-80y27r-4wvrqc-4z38tp-cdxv4k-ndfh1v-skpnxn-hd7msm-5wqb6-cvtsy3-f25ssp-hgfh9d-w1m8aa-et9569-3ayn56-bdfs18-70

gc:kj1r3z-r//g96sxe-80n95k-ttmg0k-6ri2t1-vc20ce-f8vp1s-7fbk6p-7vxiab-5mevpz-en36ac-

visual secret sharing schema

DOI: 10.48175/IJARSCT-10187

Generated hash code:



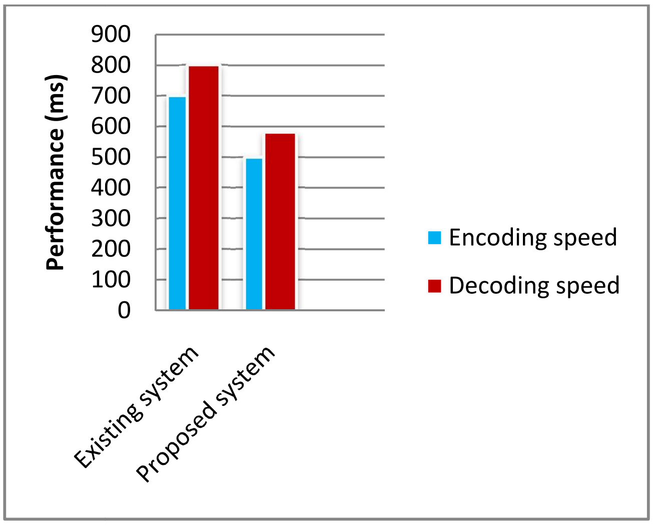
Message:

visual secret sharing schema

3750f73ed81827d4e6934c09231cbc2c

Comparison Table:

Paper	Algorithm	Encoding Speed	Decoding Speed	Security
[1]	Division, Sharing	low	low	low
This	K-means, MD5	High	high	High



Time complexity of a sharing schema algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the input.

VI. CONCLUSION

In this study, a novel DNN is built based on CNN's strong feature extraction ability, and the DNN structure is improved using tune skills such as skip connection, feature dimension reduction, feature fusion, and so on. The simulation results demonstrate that our proposed DNN has a big concealing capacity and sound hiding performance due to the architecture and loss function innovation. Our approach has a relative hiding capacity of 1 bytes/pixel, which is significantly higher than the state-of-the-art method.Hide and safeguard secret or critical military remote sensing photos is a difficult and important undertaking.

REFERENCES

[1] C. N. Yang, D. S. Wang, “Property Analysis of XOR-Based Visual Cryptography,” IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[2] Y W. Chow, W Susilo, G Yang, et al., “Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing,” Information Security and Privacy, pp.409-425, 2016.

[3] Y. C. Chen, G. Horng, D. S. Tsai, “Comment on cheating prevention in visual cryptography,” IEEE Transactions on Image-Processing A Publication of the IEEE Signal Processing Society, vol. 21, no. 7, pp. 3319-3323, 2012.

[4] P. P. Thulasidharan, M. S. Nair, “QR code based blind digital image watermarking with attack detection code,” AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.

[5] Miss A.A.NaphadeDr.R.N.khobaragadeDr.V.M.Thakare, “Improved nvss scheme for diverse image media”. International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26, 2016.

[6] P. Y. Lin, “Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code,” IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.

[7] I. Tkachenko, W. Puech, C. Destruel, et al., “Two-Level QR Code for Private Message Sharing and Document Authentication,” IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.

[8] P. Y. Lin, Y. H. Chen, “High payload secret hiding technology for QR codes,” Eurasip Journal on Image & Video Processing, vol. 2017, no. 1, pp. 14, 2017.

[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography via error diffusion”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009.

[10] Weijun Zhang, XuetianMeng,” An Improved Digital Watermarking TechnologyBased on QR Code” ICCSNT 2015.

[11] S. Mohammad Paknahad, S. Abolfazl Hosseini, Mahdi R. Alagheband,” User-friendly Visual Secret Sharing for color images Based on Random Grids” International Symposium on Communication Systems, Networks and Digital Signal Processing 2016.

[12] Deepika M P, A Sreekumar,” Secret sharing scheme using Gray code and XORoperation” IEEE 2017

[13] Javvaji V.K. Ratnam,1 P. Ramana Reddy,2 and T. Sreenivasulu Reddy3,” Design of High Secure Visual Secret Sharing Scheme for Gray Scale Images” IEEE WiSPNET 2017.

[14] Modigari Narendra1, Dhanya Ben2 C.P. Jetlin3 , Dr. L. Jani Anbarasi” An Efficient Retrieval of Watermarked Multiple Color Images using Secret Sharing” ICSCN -2017

DOI: 10.48175/IJARSCT-10187