IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Steganography System for Enhanced Security

Renuka N. Devray*, Shreya Narayan Raundal[1], Samruddhi Sunil Athare[2], Khan Umama Iliyas[3], Kakade Shubhangi Hanuman[4]
*Asst. Prof. Department of Computer Science and Design Engineering
[1,2,3,4] Student, Department of Computer Science and Design Engineering
Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar, India

Abstract: *Visual secret sharing (VSS) systems hide secret images in shares either printed on transparencies or encoded and kept digital. For further data security, we will apply security to watermarking using the NVSS technique as well as QR images and videos. Although the shares may show as meaningful images or noise-like pixels, during transmission they will cause suspicion and raise interception risk. VSS systems thus have a transmission risk issue for the secret itself as well as for the persons engaged in them. We developed a new method for secret sharing utilizing a texture and also a natural-image-based VSS scheme that shares secret images via several carrier media to safeguard the secret and the participants throughout the transmission phase in order to solve this challenge. We design the image to conceal secret messages by use of the texture generation technique. Unlike hiding messages using an existing cover image, our method hides the original texture image and embeds secret messages utilizing visual secret sharing. Natural shares could be hand-painted images in digital or physical form or photos. We also provide several approaches to conceal the secret meant to lower the share's transmission risk issue.*

Keywords: Hashing, Partitioning Algorithm, Quick Response code, Visual Secret Sharing Scheme

I. INTRODUCTION

In cryptography, secret writing is accomplished by means of enciphering and decoding of encoded signals. It is shown in cases when two people establish contact over an insecure media that can be readily listened in. Two main classes define the present encryption systems: symmetric and asymmetric encryption methods. The foundation of this classification is the function the keys serve in every algorithm. The symmetric encryption algorithms (SEA), sometimes known as secret-key encryption (SKE), demand that the message sender and the receiver both hold a shared secret key for encrypting and decryption of the message. Public key encryption, sometimes known as asymmetric encryption, (PKE) need both the message sender and the receiver to two keys in which one key is accessible to the public while the other is a private one [1]. The symmetric method proved its value and relevance as well as its capacity to fulfill needs and survive to the most recent days. Maintaining the objectives of continuous confidentiality integrity of messages and data to be transmitted and data on rest [2]. One method not requiring a key is hash cryptography. Rather, a fixed-length hash value is produced depending on the plaintext, so it is unable to be recovered for either length of the plaintext or the contents [3].

Steganography is the method of covert data concealing inside a file. The file might be video [4] or picture. The encrypted data is embedd into the underlying image using LSB method [5]. Using XOR operation between the LSB of the picture pixel value and the secret data to be hidden, this method generates The output finds place in the least significant piece of the base picture [5]. The human visual system cannot detect the variations in the base image since the total movement is negligible. This method is highly advised [5] because of its simplicity and negligible decrease in image quality. Visual Cryptography (VC) is a method wherein a secret image is encrypted into n shares, each participant possessing one or more shares. Less than n share holders cannot divulge about the secret image. Stacking the n shares exposes the secret image and the human visual system can identify it straight away [6]. Images, handwritten documents, pictures, and others are among the several kinds of secret images. A visual secret sharing (VSS) system is another name for exchanging and presenting secret images. VC's original goal was to safely distribute

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

hidden photos in noncomputer-aided settings; nonetheless, devices with computational capability are now somewhat common.

II. REVIEW OF LITERATURE

The work [1] shows how XVCS works better than OVCS and offers thorough investigation of QR based on XOR based Visual Cryptography System. The obtained contrast with XVCS is more than with OVCS. XVCS's 2^((k-1)) contrast is twice that of OVCS. For OR-based VCS, the monotone quality of OR operation compromises the visual quality of reconstructed images. Benefits include: Stack operations will help you to easily decipher the secret image. XVCS reconstructed images better than OVCS. The quality of the decrypted image is more since obtained contrast of it is more.

Author suggested in paper [2] that if necessary modifications in the QR code image will help to precisely identify the information contained in it. Thus, based on geometric classic geometric correction, it is recommended to fix the QR distortion algorithm. First, the exact coordinates of four vertices of the QR code image distortion pretreatment of QR image is obtained by following procedures. Based on coordinates obtained geometric correction is done in second stage. Third phase following correction: the QR code binary image is precisely reconstructed after black and white data block recognition and storage. That's how QR code's application area gets expanded.

Possibly utilized for document authentication, the two-level QR code (2LQR) includes two public and personal storage layers [3]. Since the general public level is the same as the standard QR code storage level; thus, any classical QR code application can be readable. Changing the black modules with particular textured patterns creates the private level. Data encoded using QR codes with error correction capability makes up it. The advantages are: It raises the QR code's storing capability. The textured patterns applied in 2LQR sensitive to the P&S process. Cons include: I have to enhance the approach of pattern identification. The storage capacity of 2LQR can be increased by replacing the white modules with textured patterns.

This paper [4] propose sharing QR code secrets explodes the error correction mechanism inherent in the structure of the QR code, for circulate and encode data about a mystery message into various activities. Each activity in the plan is developed from a QR cover code, and each offer itself is a legitimate QR code that can be examined and decoded by a QR code reader. Advantages are: The secret message can be recuperated the mystery message can be recouped by consolidating the data contained in the QR code shares. Disadvantages is: secrete sharing depends on code words.

This paper [5] propose Advanced cheating prevention mechanism to QR code. First the sender of the image shares the keys with the participants and after sending the share first participant is authenticated by using validation code and key if any of the participant is dishonest then secret decoding process stops at that point itself. Highest version of the QR code that is version 40 is used in the paper. Advantage is introduced an advanced cheating-prevention visual secret-sharing. Presented approach is tolerant to print and scan operation to protect QR data in real world application.

In paper [6] 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 [7] paper, plan a secret QR sharing way to deal with ensure the private QR information with a protected and reliable distributed system. The proposed approach contrasts from related QR code conspires in that it utilizes the QR qualities to accomplish secret sharing and can oppose the print-and-sweep activity. Advantages are: Reduces the security risk of the secret. Approach is practical. 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 scanner tag. QR system requires lessening the alterations.

In this work [8], 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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

In this paper [9], 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 [10], 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.

In this paper [11], 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 k1 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.

III. PROPOSED METHODOLOGY

Using advanced partitioning technique, a new method is shown in proposed system to increase QR Image and Video security. Loss of security affects a current sharing method. Under this assumption, consider the approach for (k, n) get to structures utilizing the (k, k) sharing occurrence on every k-member subset dependant on particular relationship. This approach will call for many examples as n increases. Thus, provides partioning computations to arrange all the k-member subsets into a few assortments, in which case one can replace cases of several subsets. The intended visual sharing schema is to conceal the secrets into a little QR tag. Furthermore able to reveal the shrouded enigma is only the authorised person carrying the private key. precisely.

A. 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.

B. Architecture

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

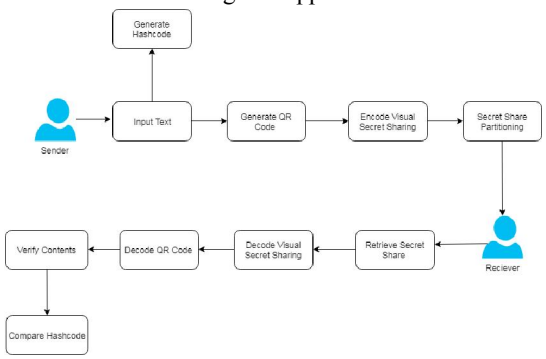


Fig. 1. Proposed System Architecture

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

C. Algorithms

1. Hashing Algorithm:

The MD algorithm is used for authentication of the message. It is a one-way cryptographic function that takes message of any length as input and generate fixed length hash value as output. The output hash generated is 128 bit key and it is impossible to generate same hash value for two messages, so it gives more secure way for authentication of message.

Steps:

A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.

The output of a message digest is considered as a digital signature of the input data.

MD5 is a message digest algorithm producing 128 bits of data.

It uses constants derived to trigonometric Sine function.

It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.

Most modern programming languages provides MD5 algorithm as built-in functions

2. K-means clustering:

K-Means Clustering is an iterative, unsupervised algorithm that is used to partition data into clusters based on the similarity present among data points. In this work K-means clustering is used in order to partition the secret message into shares so that it can be distributed to participants. In K-means data is partitioned in such a way that each data point belongs to only one group so as reduce intra-class dissimilarity and increase interclass dissimilarity. In this work for division of message into cluster, a word is compared with center of each cluster and it is then moved to the cluster in which the distance is less from the center.

Steps:

Give the number of cluster value as k.

Randomly choose the k cluster centers

Calculate mean or center of the cluster

Calculate the distance between each word to each cluster center

If the distance is near to the center then move to that cluster.

Otherwise move to next cluster.

Re-estimate the center.

Repeat the process until the center doesn't move.

3. 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.

4. 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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

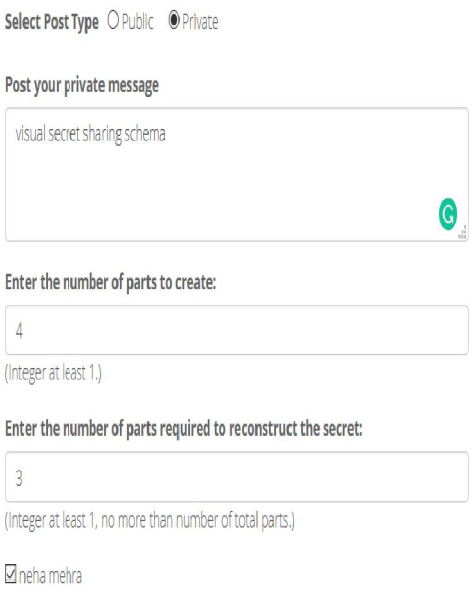
IV. RESULTS AND DISCUSSION

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.

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:

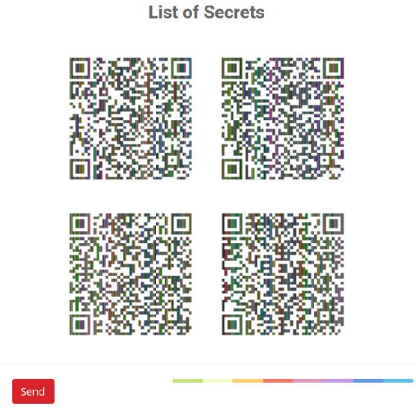
Enter message, number of parts to create, enter the number of parts required to reconstruct the secret and specific user participants.



Message – visual secret sharing schema

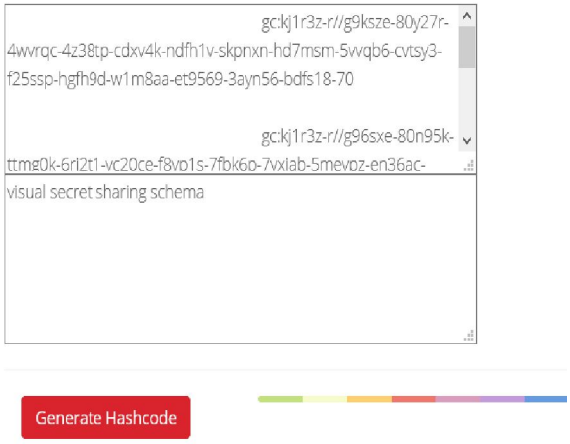
Generated Hash code of message - 3750f73ed81827d4e6934c09231cbc2c.

Generate number of Parts using advanced partitioning technique i.e. k-means clustering

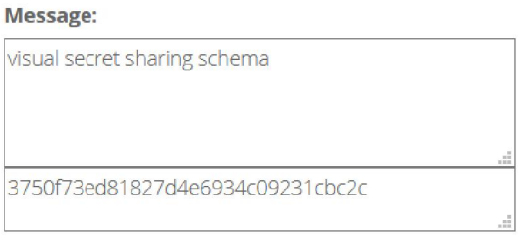


IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Receiver:
Decode Message:



Generated hash code:



V. CONCLUSION

In this paper, a visual secret sharing scheme for QR code applications, which makes improvement mainly on two aspects: higher security and partitioning techniques based on specific relationships. In addition, we extended the access structure from (n, n) to (k, n) by further investigating the error correction mechanism of QR codes. Message accuracy is checked using Hashing technique.

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]. Wang Xuan, Cao Peng, FengLiuping, Zhu Jianle, Huopeijun,"Research on Correcting Algorithm of QR Code Image's Distortion "17th IEEE International Conference on Communication Technology 2017.
[3]. I
[4]. 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.
[5]. 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.
[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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

[7]. Miss A.A.Naphade Dr. 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.

[8]. 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.

[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]. S. Mohammad Paknahad, S. AbolfazlHosseini, 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.

[11]. Deepika M P, A Sreekumar," Secret Sharing Scheme Using Gray Code and XOR Operation" IEEE 2017.

[12]. 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.