

Mobile Payment Authentication Using QR Code Based on Visual Cryptography Scheme

^{1st} Deny Ahmad Sofyan
School of Computing
Telkom University
Bandung, Indonesia

denyahmdsofyan@student.telkomuniversity.co.id

^{2nd} Satria Mandala
School of Computing
Telkom University
Bandung, Indonesia

satriamandala@telkomuniversity.ac.id

^{3rd} Erwid M Jadied
School of Computing
Telkom University
Bandung, Indonesia

jadied@telkomuniversity.ac.id

Abstract—Advances and developments in technology are used by the community to support various sectors, one of which is the payment sectors. Nowadays, people can easily make mobile payment transactions via QR Codes, such as QRIS, Go-Pay, Dana, OVO, etc. increasing the demand for information and data protection. This convenience poses many security risks in its use. Attackers can look for a crack for committing crimes on payment transactions and making a lot of businesses suffer economic losses. There are many ways that hackers can obtain information or data, so information and data need to be protected. Therefore, the development of a robust mobile payment authentication system is imperative. In this research, Visual Cryptography is proposed to secure the transaction using QR Codes using Extended Visual Cryptography Scheme (EVCS) for making the shared image into meaningful image to make it easier for the public to use the transaction. This paper uses Bit-level Visual Cryptography Scheme (VCS) and the Steganography method for the extended Visual Cryptography Scheme (EVCS) by embedding the pixel data from shared image into carrier image. The performance result from this research shows that the EVCS has the 29 Db on PSNR score and 53 % on the SSIM score while the MSE score is 84.36, also the image can be reconstructed without any problem and can be recognizable for the human vision and QR Code reader device.

Keywords—Visual Cryptography, Bit-level, EVCS, Steganography, QR Code, Authentication System

I. INTRODUCTION

Along with the technological advancements, QR code payments are now one of the most used mobile payment tools [1]. The mobile payment is a common way of quick payment used in some emerging markets [2], such as QRIS, Go-Pay, Dana, OVO, etc. increasing the demand for information and data protection [3]. With this convenience, there are still many security risks using this payment method, people want to have guaranty for them transactions. Because there are numerous ways that hackers can obtain information or data, the rapid development of the internet and technological advancements have resulted in an increase in the amount of information and data that needs to be protected [4][5]. For instance, a QR code representing the merchant's account is pasted on the wall of one of the stores. The QR code doesn't have an anti-counterfeiting feature. As a result, a thief can alter the personal information contained in the QR code using his own bank account without detection. When a transaction is made, money might be transferred to the attacker's account. To further reduce the financial harm that bad actors do to businesses and to strengthen the security of the mobile payment authentication procedure, Visual Cryptography is one of the pertinent studies that has been done on the security of the payment authentication process, particularly when it comes to QR codes.

A method known as the Visual Cryptography Scheme (VCS) can guarantee the secure transmission of private images over the Internet. Naor and Shamir proposed it in 1994 [6]. VCS separates the hidden image into numerous pieces [7]. The system can provide a straightforward and efficient

method for storage in distributed pictures while resolving the key management issue in conventional encryption. In research [2] The scheme is capable of ensuring that QR Code payments are secure. The schemes used in [2] are VCS, RS XOR mechanism, and adopt QR code error correction mechanism.

There are several schemes that can be used in VCS. This research uses Extended Visual Cryptography Scheme (EVCS). With Bit-level as schemes for a VCS (2,2)-threshold method, the Visual cryptography Scheme is expanded in this study using the Steganography technique. Compared to the random shares of regular VCS, an extended visual cryptography scheme (EVCS) is a type of VCS that consists of meaningful shares. [8].

For extend the Visual Cryptography Scheme, this paper uses the Steganography method for consisting of the meaningful share by embedding the data pixel from the shared image into carrier image without losing the original shared image data. Steganography is a technique that conceals the presence of secret data in the source data by packaging secret messages, secret holograms, or secret images [9].

A Visual Cryptography (2,2)-threshold approach with EVCS model for a payment authentication system is suggested based on the previous description. In order to acquire performance results, the model is assessed.

II. LITELATURE REVIEW

In Paper [6] Naor and Shamir explore a novel cryptographic scheme that enables the extraction of concealed images without the need for cryptographic computations. This scheme ensures perfect security and boasts a straightforward implementation.

In Paper [1] conducted research on a visual cryptography scheme with a modular approach that can listlessly secure the data included in a QR Code. The data in the QR code can be secured using this journaling approach. The share's image quality after decryption is identical to that of the original image before encryption.

In research [2], The combination of the shadow, background image, and QR code is executed using the XOR mechanism of RS, this can increase uniformity between the shadow and the QR code and improve shadow concealment. the secret information cannot be calculated iteratively using current technology.

Paper research [10] proposed a visual cryptography-based XOR scheme with a lossless reconfigurable algorithm. By comparing the secret image to n shared images, the research encrypts the secret image's color and grayscale. This research shows that the shared image does not experience pixel expansion problems.

In Paper [11] discusses research on secure QR-based online payment solutions, where the scheme can set up multiple threads on the server to detect and delete QR codes that have been stored for more than five minutes. However, the optimization of the encryption and/or decryption process is still not fast and efficient.

In paper [12] proposed research on how to provide security to QR code-based applications. With the aid of an improved (k,n) sharing algorithm [13][14], the system may save users private and public data and share it with others using a different QR code technique.

Paper Research [15] conducted research on various payment authentication methods utilizing QR codes. The findings demonstrate that shadows have become more intricate and powerful, while QR codes' security has improved. This study can strengthen security against shadow combinations' hacking of QR codes. The security of the QR code is still viewed as being less strong in this publication.

Research [16] on adaptive visual cryptography methods based on QR. The research shows that the schemes have high feasibility and robustness can be applied to share schemes for other visual cryptography not just QR codes.

In paper [17] discusses research on steganography and visual cryptography combined to provide secure transactions in online shopping. In this research, the scheme can prevent phishing in QR code hacking. However, the system still uses a simple scheme so that it can add complexity to the transaction.

This paper [18] In the proposed research, meaningless shares are produced using an optimization technique and the typical VC scheme architecture. The next stage is directly embedding cover images into each sharing using a stamping technique. The results of the experiments show that this strategy is effective in resolving the pixel expansion problem of the EVCS for GASs. Additionally, the recovered image has a display quality that is quite similar to that attained by traditional VC techniques.

III. PROPOSED SYSTEM MODEL

The system developed in this study is a system development model for Bit-level Visual Cryptography schemes (VCS) and the Steganography method for Extended Visual Cryptography Schemes (EVCS), which embed data pixels from shared images into carrier images. This allows the final shared image to be meaningfully compared to the noise image produced by the VCS. Figure 1 shows how this concept works in action.

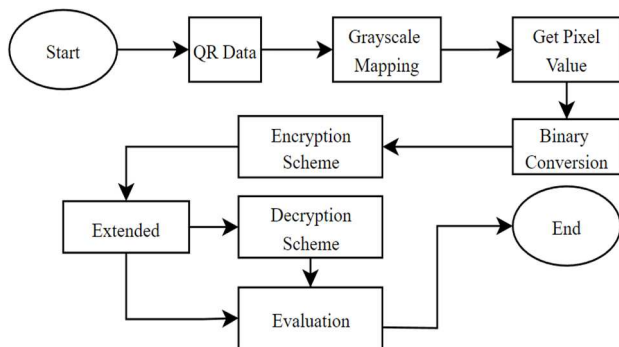

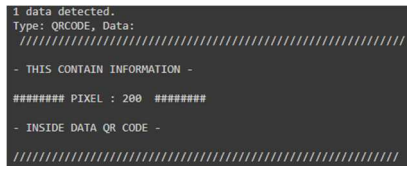


Fig. 1. System Model Flowchart.

A. QR Data

The data used in this research is a QR Code image generated in the QR Code generator software. Table I shows the secret image for the QR Code as well as the decoding information.

TABLE I. RESEARCH DATA IMAGE

QR Image	Decoded Data
	

B. GrayScale Mapping

Grayscale mapping is the next process once the data has been produced. The image's RGB pixel values are converted to grayscale via the grayscale mapping technique. It is used to shorten the running time and make the data more relevant because the data is a QR Code, which uses only two colors black and white—and the running time would be wasteful if the QR picture still employed RGB pixels. The RGB array of [255,255,255] pixels is changed to grayscale [255].

C. Binary Conversion

Binary conversion is a process to convert pixel array data. Binary conversion is used to convert pixel array data with decimal values into pixel array data with binary values. It is intended that binary values can be used as vector data in the bit-level Visual Cryptography process. For example, one of the pixel array indexes is [255] then it is transformed into [11111111].

D. Encryption Scheme

An encryption method called Visual Cryptography divides a secret image into several pieces [19]. Figure 2 illustrates how the original image will be split into n parts using various techniques. In [20] for the first time, Tuyls. introduced the concept of XOR-based Visual Cryptography Scheme (XVCS). In this research, the encryption stage uses Bit-level Visual Cryptography Scheme with (2,2)-threshold method.

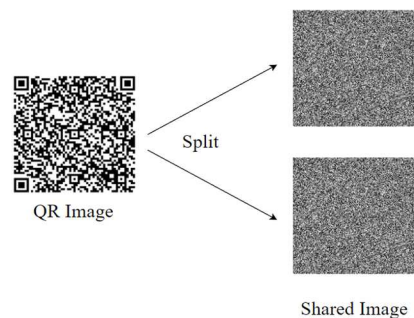


Fig. 2. Visual Cryptography Encryption.

For encrypt the secret image and generating share image, the Bit-level Scheme will get the binary matrix data from the previous stages, Following the bit value, the data will be divided into multiple pieces of matrix. Both blocks inserted in encrypted images are the same if the original image's pixel is white, and the opposite is true if the pixel is black. Based on this research [21] the encrypted image can be generated by following this Table II below:

TABLE II. (2, 2)-THRESHOLD SCHEME

Pixels	Prob	Share 1	Share 2	Stacking
<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div> White	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
Pixels	Probability	Share 1	Share 2	Stacking
<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div> Black	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>
	1/6	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>

Each pixel in the original image can be replaced by a 2 2 block of subpixels in the shared image using a (2, 2) approach. According to Table II, if the original pixel is white, one of six share pixel combinations is generated at random. For example, if the value of the pixel is (11) so the binary value is [0011110], then divide each pixel in the image C into several matrix as in the equation below:

$$[0011110] = ([S_0], [S_1]) = \left(\begin{bmatrix} 00 \\ 11 \end{bmatrix}, \begin{bmatrix} 11 \\ 10 \end{bmatrix} \right) \quad (1)$$

Where the S_0 and S_1 is the share binary value for the shared image.

E. Extended Scheme

The Bit-level Visual Cryptography strategy is enhanced utilizing the Steganography technique using the Extended Scheme. Steganography is the method of encasing discrete, secret multimedia information inside of much larger, publicly available multimedia information, such as images, text, files, or movies [22].

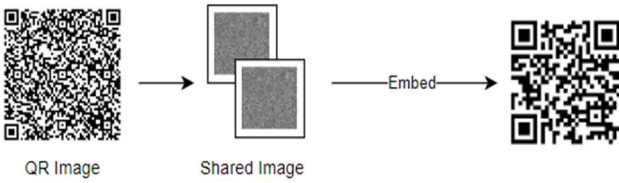


Fig. 3. Steganography Process.

In this research, as shown in Figure 3, the secret image resulting from Visual Cryptography will be manipulated so that the visible image is not a noise image. As in Cryptography, Steganography allows the hiding of a picture within another image that has been altered so that the hidden information cannot be seen [23]. The embedding process is performed by taking the shared image pixel data and storing it as an array and then inserting it into the carrier image.

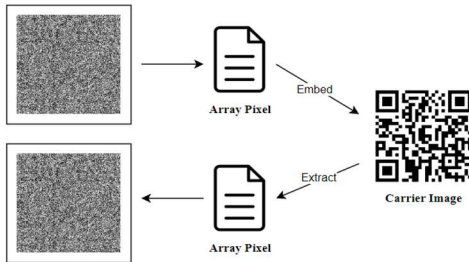


Fig. 4. Embedded Image Process.

As shown in Figure 4, the whole process both embedding and extracting the pixel data from the shared image into carrier

image by turning it into array data which can be stored into text file.

F. Image Decryption

The shared image will be combined with the retrieved original image during the image decryption process.

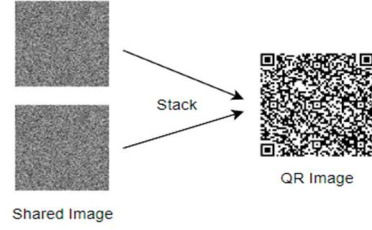


Fig. 5. Visual Cryptography Decryption.

To examine the value of the shared image and compare the pixel values from each shared image, as shown in Figure 5, shared image will be reconstructed using brute force iteration, Table III below serves as the basis for the decryption process.

TABLE III. (2,2) TRUTH TABLE DECRYPTION

Secret Pixel	White						Black					
Share 1	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
Share 2	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>
Stack Result	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: white; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 10px; height: 10px; background-color: black; border: 1px solid black;"></div>

G. Authentication System Model

Authentication System Model is proposed in this paper for securing the payment of transaction. Figure 6 below shows the whole flow of the system model.

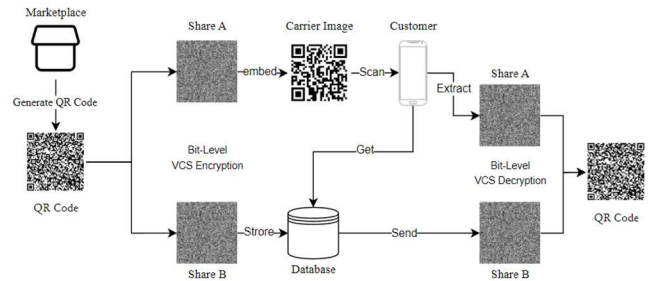


Fig. 6. Authentication System Model.

Figure 6 above shown an overview of the system design. The application will receive a scanned QR Code that contains a shadow QR Code along with a picture of the share a from the split result done by the business owner when generating a payment QR Code. Next, the application will read the share an image in the shared carrier QR Code, then the server will send the share b image to the application system for stacking where previously the share an image was stacked. Even when the server has been attacked by some hacker which is common used called DDoS, the attack causing the server to become overloaded with packet requests and function improperly [24]. The Share image can still be stacked by the user manually by uploading it and the system will generate the actual QR Code. After the system does the stacking then the system will read the QR Code as payment details.

H. Evaluation

Several testing metrics, including MSE, PSNR, SSIM, and Entropy Score, are used in this study's evaluation stage.. These

testing metrics are applied to the image encryption and description results that have been carried out. PSNR is a commonly used method to calculate the similarity of the processed image with the original image [25] which is obtained by the equation:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (2)$$

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2 \quad (3)$$

The unit of PSNR is db. The similarity between the two images increases with increasing PSNR scores. Comparing the structural similarity between the original image and the reconstructed image, SSIM is employed in an approach similar to that of PSNR [26] which is calculated by the equation :

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (4)$$

Metric Entropy is used to calculate the level of randomness of a dataset, the metric can be obtained by equation:

$$H(x) = - \sum (p(x) \times \log_2(p(x))) \quad (5)$$

IV. EXPERIMENTAL RESULT

By referring to the acquisition of scores, the assessment phase of this research is going to evaluate the effectiveness of the system that has been developed. Grayscale Mapping is the first stage of the system's construction, followed by the Generate Matrix Shared step, after which the data is encrypted using a Bit-level Visual Cryptography Scheme and the (2,2)-threshold approach. Then the Extended Scheme uses the method of Steganography by embedding the share image into the carrier image so that the data does not look like a noise image and is suspicious to hackers [27]. Data is analyzed by comparing the outcomes of encryption, data hiding, and decryption from each approach, after the secret image is decrypted using the same scheme as encryption. Three metrics will be used to test the data throughout the testing phase: PSNR, SSIM, and Entropy Score.

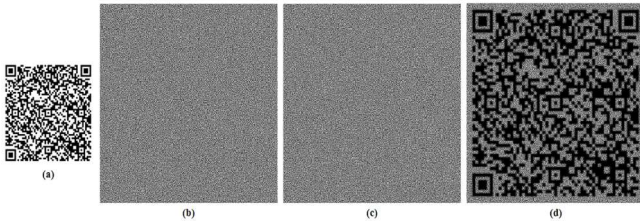


Fig. 7. (2,2)-threshold Bit-level Scheme Result

In Figure 7 shows the Figure 7(2,2)-threshold method using EVCS scheme where Figure 7(a) is the original QR code image, Figure 7(b-c) is the encrypted image, and Figure 7(d) is the reconstructed image. Table IV below shows the test results of the performance analysis for each scheme and method.

TABLE IV. PERFORMANCE ANALYSIS RESULT

Scheme	Method	MSE	PSNR	SSIM	Avg. Entropy
Bit-level VCS	(2,2)-threshold	84.21	29 dB	53 %	7.98

Table IV above shows the results of Bit-level Scheme by comparing the recovery image and the secret image (original QR Code) produces the MSE, PSNR, and SSIM scores which are 84.21 for the MSE score, 29 dB for PSNR score, it because the shared image is 2 times larger than the original image because of pixel expansion and 53 % for the SSIM score because the recovery image has the threshold shadow for the result. For the average entropy score Bit-level Scheme produces high randomness score for the sharing image, that is proved by produces the average score 7.98 which means that the Bit-level Scheme is able to generate highest random values in a shared images matrix.

TABLE V. PIXEL EXPANSION RESULT

Scheme	Method	Pixel Expansion	Expansion Size
Bit-level VCS	(2,2)-threshold	yes	4

Table V demonstrate the bit-level scheme has a pixel expansion with the size is 4 as that is caused the performance for the recovery proses which has an effect on the different structural from the secret image, it has proven by the result of the performance analysis on the Table V, it shows that bit-level scheme has big MSE score 84.21 that's caused the PSNR and SSIM score to low result.

The scheme can encrypt the secret image and split into two (2,2) sharing images and reconstruct the share image without any problem, also can be recognizable for the human vision and QR code reader device. The results demonstrate that the bit-level scheme has pixel expansion, and since the bit-level scheme is represented by the (2,2)-threshold approach, sharing images are now twice as large as the original image due to the threshold [28]. For the bit-level scheme's performance evaluation, this paper use three metric which are MSE, PNSR, and SSIM score to determine the quality of each scheme and method, the paper also use Entropy score to calculate the average randomness score of the generated shared image.



Fig. 8. Extended Scheme Result

In Figure 8 shows that the Extended Scheme using Steganography method, where Figure 8(a-b) is the carrier image and carrier image after Steganography, Figure 8(c-d) is the decode data for carrier image before and after Steganography. The method is able to hide the image share data by turn the pixel data form the shared image into an array and inserting it in the carrier image, this is shown in Figure 6(b) the image decode result shows the same data as the carrier image in Figure 6(a) before Steganography. Table VI below displays the outcomes of the test by contrasting the carrier QR image with the carrier QR image following steganography using MSE, PSNR, and SSIM.

TABLE VI. TEST RESULT STEGANOGRAPHY

Scheme	MSE	PSNR	SSIM
EVCS	0.19	55.36 dB	99%

From the Table VI, the results of Extended Scheme by compared the final shared image after Steganography method and the recovery image from Bit-level Scheme produce the score on PSNR is 55.36 dB and SSIM is 99% because of the MSE score from the scheme is resulting 0.19 which mean the final shared image after Steganography is same close as the carrier image, even almost no difference.

Figure 9 shows that the recovery image after the Extended Scheme process using Steganography, where Figure 9(a) is the share image from Bit-level Scheme, Figure 9(b) is the final shared image by Extended Scheme, and Figure 9(c) is the recovery share image from Extended Scheme. Table VII below shows the results of the comparative testing between the final sharing image and recovery image following the Extended Scheme process.



Fig. 6. Hiding Data Recovery Result

TABLE VII. RECOVERY RESULT STEGANOGRAPHY

Scheme	Method	MSE	PSNR	SSIM
EVCS	Steganography	0.0	∞ dB	100%

From Table VII above, the results of Extended Scheme after recovery from Steganography show that the share image of the scheme and the image of the Steganography recovery have similar image values and also no differences between the two images. This is proven by the perfect MSE, PSNR, and SSIM scores, the scheme obtains a score of MSE 0, PSNR ∞ dB and SSIM 100%.

V. COMPARISON TO OTHER SCHEME

In this section, the schemes from other research will be compared to this paper.

TABLE VIII. PERFORMANCE ANALYSIS RESULT

Scheme	PSNR	SSIM	Pixel Expansion	Expansion Size
MEVSS [29]	∞ dB	100%	No	0
XVCS [10]	∞ dB	100%	No	0
HP-VCS [30]	52 dB	23%	No	0
EVCS	29 dB	53 %	Yes	4

As shown in Table VIII, the MEVSS and XVCS schemes have high PSNR and SSIM values because the contrast in the VCS while the threshold is not limited and does not have pixel expansion, but the HP-VCS and EVCS have low PSNR and SSIM values because the threshold is limited, also the EVCS has the pixel expansion with size 4.

For the EVCS, this scheme has meaningful shared image even has the pixel expansion compared to HP-VCS which does not have the pixel expansion, Although the HP-VCS has

low SSIM score while the image should be as similar as possible to the original image because payment authentication system based on QR Code is using the image for the model system design.

The MEVSS and XVCS is not recommended for this paper that because the result image from the encryption prosses is not meaningful, which means the image cannot be scanned by any QR Code reader because the image can only be seen as noise image that's make low performance compared to EVCS and HP-VCS which that scheme have meaningful share image so can be scanned by any QR Code reader.

VI. CONCLUSION

Based on the results of the research for the Mobile Payment Authentication Using QR Code based on Visual Cryptography Scheme, tests, analyses, and the results were conducted, It uses a Bit-level Visual Cryptography approach for the encryption and decryption processes, and for the Extended Scheme, this work uses Steganography to embed the pixel data to carrier image so the final shared image is not like the noise image also securing data image from attacker. the conclusions are as follows. Any Image can be split into two pieces without revealing any information in the shared image, it also can be recognizable for the human vision and QR Code reader device.

For the performance analysis of Bit-level Scheme resulting the reconstructed image from Bit-level Visual Cryptography Scheme is not have the similar structure as the secret image, it is because the high MSE score of the scheme is 84.21 caused the low score of PSNR and SSIM which are 29 dB and 53%, but in the average entropy score of the share image, the EVCS has the high score which is 7.98. In Bit-level Scheme the reconstructed image has pixel expansion with size is 4.

For the Extended Scheme, the data pixel of the shared image from Bit-level Scheme can be stored without revealing information inside the carrier image, for the performance analysis the EVCS has score on PSNR is 29 dB and SSIM is 53% because of the MSE score from the scheme is resulting 84.21 which is low. For the recovered image, the EVCS can produce the MSE, PSNR, and SSIM scores, which are MSE 0, PSNR ∞ dB and SSIM 100%.

The MEVSS and XVCS is not recommended for the payment authentication system based on QR Code image because the result image from the encryption prosses is not meaningful, but for the EVCS, this scheme has meaningful shared.

Suggestions for further research are to use different Visual Cryptography Scheme, and may also can use different methods for securing the shared image. Besides that, this system model can be implemented into software or app development.

REFERENCES

- [1] D. B. Dananjaya, "Pengamanan Quick Response (QR) Code Berbasis Skema Kriptografi Visual," Makal. IF4020 Kriptografi, 2022.
- [2] J. Lu, Z. Yang, W. Yuan, L. Li, C. C. Chang, and L. Li, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," Mob. Inf. Syst., vol. 2017, pp. 1–13, 2017, doi: 10.1155/2017/4356038.
- [3] S. Mandala, A. I. Ramadhan, M. Rosalinda, S. M. Zaki, and E. Weippl, "DDoS Detection Using Information Gain Feature Selection and Random Forest Classifier," in 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Dec. 2022, pp. 294–299. doi: 10.1109/ICICyTA57421.2022.10038126.

- [4] S. Mandala, A. I. Ramadhan, M. Rosalinda, W. M. . Yafooz, and R. H. Khohar, "DDoS Detection by Using Information Gain-Naïve Bayes," in 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Dec. 2022, pp. 283–288. doi: 10.1109/ICICyTA57421.2022.10038054.
- [5] S. Mandala, M. A. Ngadi, J. M. Sharif, M. S. M. Zahid, and F. Mohamed, "Investigating severity of blackhole attack and its variance in wireless mobile ad hoc networks," *Int. J. Embed. Syst.*, vol. 7, no. 3/4, p. 296, 2015, doi: 10.1504/IJES.2015.072370.
- [6] Ashutosh and S. D. Sen, "Visual cryptography," *Proc. - 2008 Int. Conf. Adv. Comput. Theory Eng. ICACTE 2008*, pp. 805–807, 2008, doi: 10.1109/ICACTE.2008.184.
- [7] L. Ren and D. Zhang, "A QR code-based user-friendly visual cryptography scheme," *Sci. Rep.*, vol. 12, no. 1, pp. 1–8, 2022, doi: 10.1038/s41598-022-11871-9.
- [8] T. Prem Jacob, A. Pravin, and P. Asha, "Embedded Extended Visual Cryptography," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 26, pp. 1233–1240, 2019. doi: 10.1007/978-3-030-03146-6_144.
- [9] U. K. Mondal, S. Pal, A. R. Dutta, and J. K. Mandal, "A New Approach to Enhance Security of Visual Cryptography Using Steganography (VisUS)," *arXiv Prepr. arXiv2103.09477*, 2021, [Online]. Available: <https://arxiv.org/abs/2103.09477> <https://arxiv.org/pdf/2103.09477>
- [10] H. Wang, Z. Jiang, Q. Qian, and H. Wang, "An efficient XOR-based visual cryptography scheme with lossless reconfigurable algorithms," *Int. J. Distrib. Sens. Networks*, vol. 18, no. 4, 2022, doi: 10.1177/15501329221084223.
- [11] L. Ahmad, R. Al-Sabha, and A. Al-Haj, "Design and Implementation of a Secure QR Payment System Based on Visual Cryptography," *2021 7th Int. Conf. Inf. Manag. ICIM 2021*, no. 07, pp. 40–44, 2021, doi: 10.1109/ICIM52229.2021.9417129.
- [12] S. Laiphrakpam and D. B. Gothawal, "Implementation of Security Scheme for QR code based Application with Enhanced (k, n) sharing Approach," vol. 6, no. 6, pp. 9–17, 2019.
- [13] S. Mandala, A. R. Pratiwi Wibowo, Adiwijaya, Suyanto, M. S. M. Zahid, and A. Rizal, "The Effects of Daubechies Wavelet Basis Function (DWBf) and Decomposition Level on the Performance of Artificial Intelligence-Based Atrial Fibrillation (AF) Detection Based on Electrocardiogram (ECG) Signals," *Appl. Sci.*, vol. 13, no. 5, p. 3036, Feb. 2023, doi: 10.3390/app13053036.
- [14] S. Pa, S. Mandala, and Adiwijaya, "A new method for congestion avoidance in wireless mesh networks," *J. Phys. Conf. Ser.*, vol. 1192, p. 012062, Mar. 2019, doi: 10.1088/1742-6596/1192/1/012062.
- [15] L. Li et al., "Multiple schemes for bike-share service authentication using QR code and visual cryptography," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11065 LNCS, pp. 629–640, 2018, doi: 10.1007/978-3-030-00012-7_57.
- [16] L. N. Zhang, C. Y. Cui, X. Y. Zhang, and W. Wu, "Adaptive visual cryptography scheme design based on QR codes," *Math. Biosci. Eng.*, vol. 19, no. 12, pp. 12160–12179, 2022, doi: 10.3934/mbe.2022566.
- [17] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," *2014 IEEE Students' Conf. Electr. Electron. Comput. Sci. SCEECs 2014*, vol. IV, no. X, pp. 94–96, 2014, doi: 10.1109/SCEECs.2014.6804449.
- [18] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1 PART 2, pp. 219–229, 2012, doi: 10.1109/TIFS.2011.2167611.
- [19] D. R. Ibrahim, J. Sen Teh, and R. Abdullah, "An overview of visual cryptography techniques," *Multimed. Tools Appl.*, vol. 80, no. 21–23, pp. 31927–31952, 2021, doi: 10.1007/s11042-021-11229-9.
- [20] P. Tuyls, H. D. L. Hollmann, J. H. Van Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes," *Des. Codes, Cryptogr.*, vol. 37, no. 1, pp. 169–186, 2005, doi: 10.1007/s10623-004-3816-4.
- [21] I. Canadian, C. Of, and E. Engineering, "AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES N. Askari, H. M. Heys, and C. R. Moloney Electrical and Computer Engineering Faculty of Engineering and Applied Science Memorial University of Newfoundland," 2013.
- [22] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.
- [23] H. Shi, X. Y. Zhang, S. Wang, G. Fu, and J. Tang, "Synchronized Detection and Recovery of Steganographic Messages with Adversarial Learning," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11537 LNCS, pp. 31–43, 2019, doi: 10.1007/978-3-030-22741-8_3.
- [24] L. W. P. Adi, S. Mandala, and Y. Nugraha, "DDoS Attack Detection System using Neural Network on Internet of Things," in 2022 International Conference on Data Science and Its Applications (ICoDSA), Jul. 2022, pp. 41–46. doi: 10.1109/ICoDSA55874.2022.9862848.
- [25] D. A. N. Sauvola et al., "PERBAIKAN CITRA TANDA TANGAN DIGITAL MENGGUNAKAN METODE OTSU THRESHOLDING DAN SAUVOLA," vol. 25, no. 1, pp. 28–34, 2023.
- [26] A. M. Ragab and M. El Khouly, "Gray Visual Cryptography Algorithm for Secret Sharing," *Int. J. Comput. Sci. Mob. Comput.*, vol. 9, no. 7, pp. 154–166, 2020, doi: 10.47760/ijcsmc.2020.v09i07.001.
- [27] A. J. Parsaoran, S. Mandala, and M. Pramudyo, "Study of Denoising Algorithms on Photoplethysmograph (PPG) Signals," in 2022 International Conference on Data Science and Its Applications (ICoDSA), Jul. 2022, pp. 289–293. doi: 10.1109/ICoDSA55874.2022.9862918.
- [28] D. Taghaddos and A. Latif, "Visual cryptography for gray-scale images using bit-level," *J. Inf. Hiding Multimed. Signal Process.*, vol. 5, no. 1, pp. 90–97, 2014.
- [29] L. Yu, L. Liu, Z. Xia, X. Yan, and Y. Lu, "Lossless and efficient secret image sharing based on matrix theory modulo 256," *Mathematics*, vol. 8, no. 6, pp. 1–17, 2020, doi: 10.3390/math8061018.
- [30] D. Zhang, H. Zhu, S. Liu, and X. Wei, "HP-VCS: A high-quality and printer-friendly visual cryptography scheme," *J. Vis. Commun. Image Represent.*, vol. 78, no. April, p. 103186, 2021, doi: 10.1016/j.jvcir.2021.103186.