mathematics

MDPI

Article

An Efficient Visually Meaningful Quantum Walks-Based Encryption Scheme for Secure Data Transmission on IoT and Smart Applications

Ahmed A. Abd El-Latif [1,*], Abdullah M. Iliyasu [2,3,4] and Bassem Abd-El-Atty [5]

[1] Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[2] Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; a.iliyasu@psau.edu.sa
[3] School of Computing, Tokyo Institute of Technology, Yokohama 226-8502, Japan
[4] School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China
[5] Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt; bassem.abdelatty@fci.luxor.edu.eg
* Correspondence: a.rahiem@gmail.com or aabdellatif@nu.edu.eg

Abstract: Smart systems and technologies have become integral parts of modern society. Their ubiquity makes it paramount to prioritise securing the privacy of data transferred between smart devices. Visual encryption is a technique employed to obscure images by rendering them meaningless to evade attention during transmission. However, the astounding computing power ascribed to quantum technology implies that even the best visually encrypted systems can be effortlessly violated. Consequently, the physical realisation quantum hardware portends great danger for visually encrypted date on smart systems. To circumvent this, our study proposes the integration of quantum walks (QWs) as a cryptographic mechanism to forestall violation of the integrity of images on smart systems. Specifically, we use QW first to substitute the original image and to subsequently permutate and embed it onto the reference image. Based on this structure, our proposed quantum walks visually meaningful cryptosystem facilities confidential transmission of visual information. Simulation-based experiments validate the performance of the proposed system in terms of visual quality, efficiency, robustness, and key space sensitivity, and by that, its potential to safeguard smart systems now and as we transition to the quantum era.

Keywords: visual cryptography; quantum computing; IoT applications; quantum walks; smart systems; cyberphysical systems

Citation: El-Latif, A.A.A.; Iliyasu, A.M.; Abd-El-Atty, B. An Efficient Visually Meaningful Quantum Walks-Based Encryption Scheme for Secure Data Transmission on IoT and Smart Applications. *Mathematics* **2021**, *9*, 3131. https://doi.org/10.3390/math9233131

Academic Editor: Angel Martín-del-Rey

Received: 28 October 2021
Accepted: 28 November 2021
Published: 4 December 2021

1. Introduction

Smart systems are becoming integral parts of modern life, where they facilitate important internet-based services ranging from Internet of Things (IoT) to cloud storage, and many others. Sadly, this utility has propelled criminal activities to violate the integrity and confidentiality of the systems [1,2]. Cryptosystems, such as data hiding, and encryption protocols are reputed for tamper-proof security for several types of data [3–5]. Whereas data encryption is primarily aimed at transforming data into unintelligible formats [6,7], visual cryptography is tailored towards safeguarding the data while retaining its meaningful state [8–10]. This ability to convert confidential data into secure but meaningful forms makes visual cryptography attractive in modern cryptographic applications [11].

Generally, the visual cryptographic algorithm consists of two phases: pre-encryption and embedding phases. In the pre-encryption, confidential data is permutated, substituted, and embedded onto a reference object [12].

Recently, many visually meaningful image encryption techniques have been proposed [13–19], of which most are based on mathematical models where some information about the reference image is required during the decryption process. In the meantime, the inevitable realisation of quantum hardware means its astounding computing power could be exploited to violate the integrity and confidentiality of even the best cryptosystems [20]. To forestall this, quantum technology must be suffused into such systems. Quantum walks (QWs), which are the quantum equivalents of traditional (i.e., classical) random walks, exhibit remarkable stability and exhibit theoretically infinite key space allowances, properties that imbue them with robustness to resist diverse types of attacks [21].

Our study is primarily aimed at exploiting these properties to enhance the security of visual information on smart systems and devices. Furthermore, with necessary adjustments, our visual cryptosystem can be useful in safeguarding both pre- and post-quantum era smart systems. Similar efforts to employ QWs have been reported in, for example, Ref. [22], where Su and Wang presented a visual image cryptosystem that combined controlled QWs and single value decomposition (SVD). However, the performance of their protocol is impeded when the length of the controlling bit string is less than the number of nodes at the circle [21]. In this study, we ameliorate the zero probabilities associated with this by encrypting visually meaningful images with the QW prior to transmission in smart system frameworks. This way, our proposed system forestalls occurrence of zero probabilities. Furthermore, we use the QW to substitute the original image and permutate it whilst the substituted image is embedded onto the reference image via substitution of two least significant bits (LSBs) in the reference image. Moreover, using a pre-encryption phase, QWs ensure that the permutation and embedding processes are executed in one step.

To recapitulate, the main contributions of our study include:

1. Introducing a new visual cryptographic mechanism that exploits quantum technologies to safeguard smart systems.
2. Enhancing existing cryptosystems to overcome the weaknesses ascribed to zero probabilities exhibited when operating QWs on a circle of N vertices where the length of the controlling bit string is less than the number of nodes at the circle,
3. Utilising quantum walks (QW) first to substitute the original image and then to subsequently permutate and embed it onto the reference image, and
4. Integrating QWs into the encryption of visually meaningful images for secure transmission of sensitive data on smart systems.

To deliver the enumerated contributions, the rest of the paper is structured as follows: the layout of our proposed framework for confidential data transmission in smart systems is presented in Section 2, while essential precepts of QWs, which is the core of the proposed framework, are highlighted in Section 3. The foundations built in these two sections are subsequently used to construct algorithmic protocols of our visually meaningful encryption system whose details are presented and discussed in Section 4. Finally, outcomes of simulation-based experiments to assess the performance of the proposed method are reported in Section 5.

2. Proposed Framework for Secure Data Transmission in Smart Systems

With increased access and lower cost, cloud computing is becoming a basic computing platform in most domains of our daily lives. However, secure transfer of data between cloud computing platforms and Internet of Things (IoT) nodes (or devices) is still an important problem; more so, since there is still no standard medium to transfer data securely between and within smart systems [23,24]. Consequently, the need to develop more advanced techniques to safeguard data accessible to smart systems is a priority that cannot be overlook.

Meanwhile, the renewed interest and funding aimed at the realisation of physical quantum hardware portend great danger to today's information security architectures. The anticipated perils range from exploiting critical vulnerabilities in cybersecurity to those anticipated as we make the inevitable transition to the quantum computing era.

Both risks demonstrate the need to design efficient mechanisms for data protection and processing [4]. Failure to do so exposes smart systems and the data they transmit to unimaginable consequences related to privacy violation, impersonation, counterfeiting, etc. Using quantum technology to embed traditional cryptosystems, these expected criminal activities can be forestalled. Meanwhile, the quantum era will herald upgrades to subsisting data processing models, security standards, and available information technologies. In this regard, with minor necessary adjustments it is expected that our proposed system will be ready to secure such infrastructure on the new computing paradigm. Consequently, we introduce a new framework for confidential transmission of data on smart systems based on quantum walks whose envisioned architecture is presented in Figure 1.

Quantum walks is employed to safeguard data confidentiality and withstand probability attacks that could impugn data integrity and privacy in both traditional and quantum computing frameworks. Our proposed scheme offers a veritable structure to encrypt the secret data before uploading it to the cloud system, while the same QWs paired with correct secret keys facilitate recovery of confidential data during the decryption process.

As the core element of our proposed scheme, essential precepts of quantum walks are highlighted in the next section.

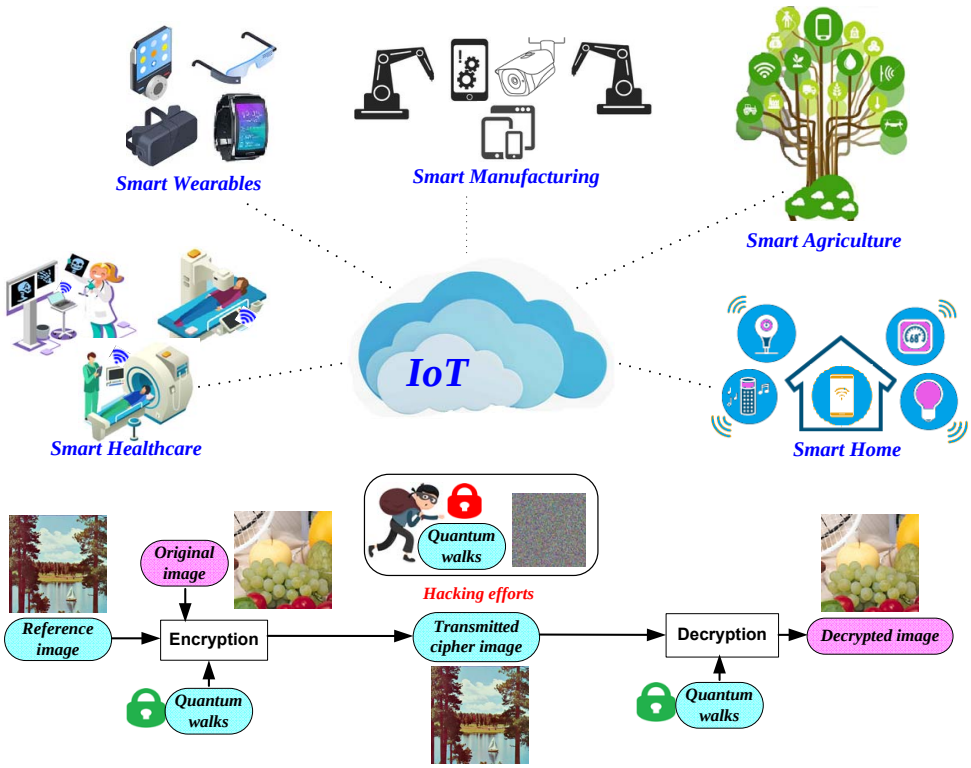


Figure 1. Illustration of framework for secure data on smart systems based on quantum walks.

3. Quantum Walks (QW)

Quantum walks (QWs) are the quantum versions of classical random walks that consist of two elements: the first element is the walker space H_s and the second one is the coin particle $H_p = \cos\beta|0\rangle + \sin\beta|1\rangle$ both H_s and H_p reside in a Hilbert space $H_s \otimes H_p$ [25]. For each step of running QW on a cycle of N vertices with a binary string T, a unitary transformation $\hat{U}_0$ ($\hat{U}_1$) is performed when the ith-bit of T is 0 (1), while the unitary transformation $\hat{U}_2$ is performed when the running step (i.e., the ith-step) is higher than the bit length of T [21]. The unitary transformation $\hat{U}_0$ can be identified in Equation (1).

$$\hat{U}_0 = \hat{F}(\hat{I} \otimes \hat{C}_0) \tag{1}$$

where $\hat{F}$ represents the shift operator of operating QW on a circle, which can be identified in Equation (2),

$$\hat{F} = \sum_{r}^{N}(|(r+1)modN, 0\rangle\langle r, 0| + |(r-1)modN, 1\rangle\langle r, 1|) \tag{2}$$

and $\hat{C}_0$ is 2×2 coin operator as presented in Equation (3) [21].

$$\hat{C}_0 = \begin{pmatrix} \cos\ \theta_0 & \sin\ \theta_0 \\ \sin\ \theta_0 & -\cos\ \theta_0 \end{pmatrix} \tag{3}$$

Similarly, $\hat{U}_1$ and $\hat{U}_2$ can be constructed as outlined for $\hat{U}_0$. After running the QW for S steps, the probability of detecting the walker at position r can be calculated as given in Equation (4).

$$\begin{aligned} P(r, S) = & \sum_{b\in\{0,1,2\}} \left|\langle r, 0|\left(\hat{U}_b\right)^S|\psi\rangle_{\text{initial}}\right|^2 \\ & + \sum_{b\in\{0,1,2\}} \left|\langle r, 1|\left(\hat{U}_b\right)^S|\psi\rangle_{\text{initial}}\right|^2 \end{aligned} \tag{4}$$

where $|\psi\rangle_{\text{initial}}$ is the initial state of QW.

Meanwhile, exploiting the outlined properties of QW and the potency of other quantum computing operations, algorithmic protocols to execute our cryptosystem to safeguard the smart systems as envisioned in Figure 1 are presented in the next section.

4. Proposed Encryption Approach

This section illuminates the role of QW in designing a new visually meaningful image encryption scheme. In the proposed encryption scheme, QW is first used to substitute the pristine (i.e., original) image, and it is also used to permutate and embed the substituted image onto the reference image by locating the pixel position in the reference image. Specifically, the substituted bits in the two LSBs of the located pixel are subsequently embedded onto the reference image. Figure 2 presents the outline of the encryption encryption and decryption phases of our scheme. The encryption process executed via steps enumerated in the sequel and outlined in Algorithm 1.

1. Select initial key parameters $(T, N, S, \beta, \theta_0, \theta_1, \theta_2)$ that can be used to run QW for S steps on a cycle of N odd vertices ruled with a binary string T to initialise an N-dimensional probability distribution vector P. Where the primary state of the coin particle is $H_p = \cos\beta|0\rangle + \sin\beta|1\rangle$ and the unitary transformations $\hat{U}_0$, $\hat{U}_1$, and $\hat{U}_2$ are constructed by θ_0, θ_1, and θ_2, respectively, $(0 \leq \beta, \theta_0, \theta_1, \theta_2 \geq \pi/2)$.
2. Retrieve the dimensionsl of the original image (OImg).

$$[x, y, z] \leftarrow size(OImg)$$

3. Reconfigure the probability vector (P) to a matrix, then alter the size of the generated matrix to the size of the original image.

$$Pf \leftarrow P(1 : fix(\sqrt{N}) \times fix(\sqrt{N}))$$

$$PK \leftarrow reshape(Pf, fix(\sqrt{N}), fix(\sqrt{N}))$$

$$RK \leftarrow resize(PK, [x, y \times z])$$

4. Reshape the matrix RK into an $x \times y \times z$ dimensional matrix and then convert the output into integers.

$$K \leftarrow reshape(RK, x, y, z)$$

$$Key \leftarrow fix(K \times 10^{12} \mod 256)$$

Algorithm 1: Encryption processes.

Input: Original image (*OImg*) and Reference image (*RImg*)
Parameters: $T, N, S, \beta, \theta_0, \theta_1, \theta_2$
Output: Encrypted image (*EImg*)

$P \leftarrow QW(T, N, S, \beta, \theta_0, \theta_1, \theta_2)$ // Use the initial key parameters for running QW for S steps on a cycle of N odd vertices ruled with a binary string T to originate a probability distribution vector P of dimension N. Where the primary state of the coin particle is $H_p = \cos\beta|0\rangle + \sin\beta|1\rangle$ and the unitary transformations $\hat{U}_0$, $\hat{U}_1$, and $\hat{U}_2$ are constructed by θ_0, θ_1, and θ_2, respectively, $(0 \leq \beta, \theta_0, \theta_1, \theta_2 \geq \pi/2)$

$[x, y, z] \leftarrow size(OImg)$ // Get the dimensional of the original image

$Pf \leftarrow P(1 : fix(\sqrt{N}) \times fix(\sqrt{N}))$

$PK \leftarrow reshape(Pf, fix(\sqrt{N}), fix(\sqrt{N}))$ // Reshape the probability vector to a matrix

$RK \leftarrow resize(PK, [x, y \times z])$ // Alter the size of the matrix PK to the size of the original image

$K \leftarrow reshape(RK, x, y, z)$ // Reshape the matrix RK to a matrix of dimension $x \times y \times z$

$Key \leftarrow fix(K \times 10^{12} \mod 256)$ // Convert the K matrix into integers

$SImg \leftarrow Key \oplus OImg$ // Substitution process

$R \leftarrow resize(P, [2x + 2y, 1])$ // Resize the probability vector P

$A \leftarrow order(R(1 : 2x))$ // Arrange the elements in ascending sequence

$XR \leftarrow index(R(1 : 2x), A)$ // Get the index of every element of $R(1:2x)$ in A

$B \leftarrow order(R(2x + 1 : 2x + 2y))$

$YR \leftarrow index(R(2x + 1 : 2x + 2y), B)$

$XImg \leftarrow expand(SImg)$ // Expand the substituted image $SImg$ of 8-bit and $x \times y$ dimension to an image of 2-bit and $2x \times 2y$ dimension

// Permutation and embedding process

for $i \leftarrow 1$ ***to*** $2x$ **do**
  for $j \leftarrow 1$ ***to*** $2y$ **do**
    $EImg(XR(i), YR(j), :) \leftarrow$ Replace 2LSBs of *RImg*(XR(i), YR(j), :) with 2bits of *XImg*(i,j,:)

5. Substitute the original image using the generated integers.

$$SImg \leftarrow Key \oplus OImg$$

6. Embed the substituted image (*SImg*) onto the reference image (*RImg*) using the following steps:
   (a) Resize the probability vector P to a vector of size $2x + 2y$.

$$R \leftarrow resize(P, [2x + 2y, 1])$$

   (b) Arrange the elements of the vector R in ascending order.

$$A \leftarrow order(R(1 : 2x))$$

   (c) Retrieve the index of every element of $R(1 : 2x)$ in A.

$$XR \leftarrow index(R(1 : 2x), A)$$

(d) Repeat the last two substeps to generate YR sequence.

$$B \leftarrow order(R(2x+1:2x+2y))$$

$$YR \leftarrow index(R(2x+1:2x+2y), B)$$

(e) Expand the 8-bit and $x \times y$ dimension substituted image $SImg$ of to a 2-bit and $2x \times 2y$ dimension image.

$$XImg \leftarrow expand(SImg)$$

(f) Replace 2LSBs of $RImg$(XR(i), YR(j), :) with 2bits of $XImg$(i, j, :) as the visual encrypted image $EImg$ (XR(i), YR(j), :) for i = 1, 2, . . . , $2x$ and j = 1, 2, . . . , $2y$.

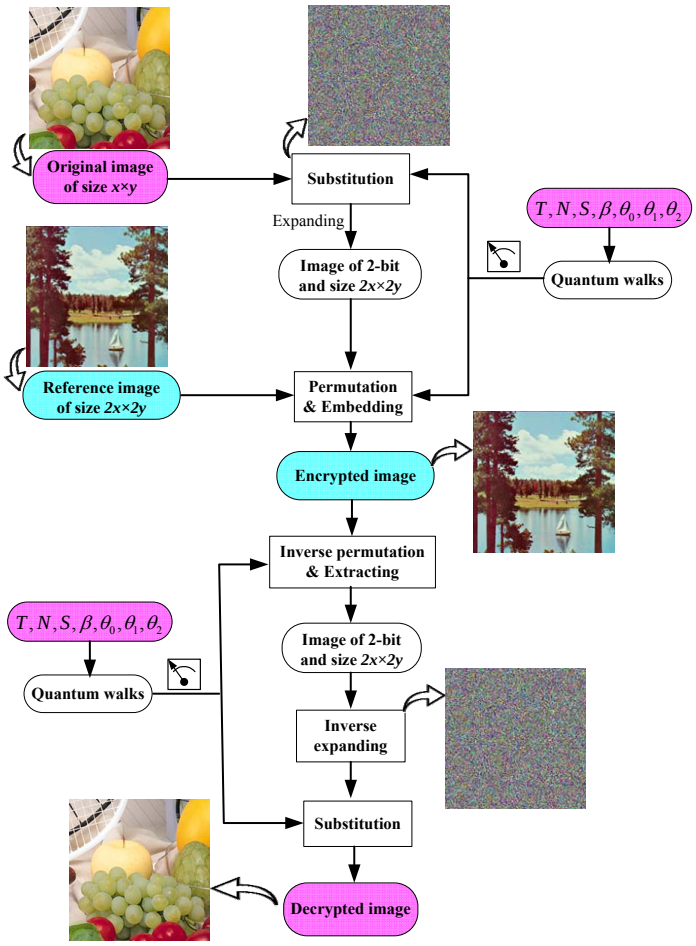


Figure 2. The outline of the presented visually encryption approach.

5. Simulation Results

To evaluate the efficiency of the proposed visually encryption method, we simulated its execution on an Intel® core^{TM} i5 and 6-GB RAM laptop computer equipped with MATLAB R2016b software. Furthermore, we used images sourced from the Signal and Image Processing Institute (SIPI) [26], Laboratory for Image & Video Engineering (LIVE) [27], and Medical Image Database (MedPix) [28] as our experimental dataset samples of which are presented in Figures 3 and 4. Images in Figure 3 labelled as OImg01 through OImg06 are 256 × 5256-dimension images used as original (or confidential) images. Similarly, images in Figure 4 labelled as RImg01 through RImg04 are 512 × 5512-dimension images used as reference images. Additionally, the key parameters used for running our QW are set

as (N = 261, S = 521, T = "0101 1001 0110 1000 1011 0001 1101 0101 0111 0111 0011 0101", $\beta = \pi/2$, $\theta_0 = \pi/4$, $\theta_1 = \pi/6$, and $\theta_2 = \pi/3$).

The remainder of the section presents outcomes of our performance analysis covering tests for visual quality, efficiency, correlation, robustness, and key space that are employed to validate advanced cryptosystems, and later we compare some of these performances with those reported in recent similar techniques.

(**a**) OImg01 (Butterfly) (**b**) OImg02 (Fruits) (**c**) OImg03 (House)

(**d**) OImg04 (Boat) (**e**) OImg05 (Bridge) (**f**) OImg06 (Scan)

Figure 3. Original images (**a**–**f**) each of size 256 × 256 used to validate the proposed scheme.

(**a**) RImg01 (Peppers) (**b**) RImg02 (Lake) (**c**) RImg03 (Baboon) (**d**) RImg04 (Plane)

Figure 4. Reference images (**a**–**d**) each of size 512 × 512 used to validate the proposed scheme.

5.1. Visual Quality Tests

The visual quality of an encrypted image is a useful tool to assess the efficiency of any visually meaningful encryption mechanism. Outcomes of encrypted images emanating from our proposed technique are reported in Figures 5 and 6, and visual inspection of those images establishes their imperceptibility and good visual quality. However, to quantitatively validate this performance, we employed the standard visual metrics of peak signal to noise ratio (PSNR) and Structural Similarity Index Metric (SSIM). These metrics can be formulated as presented in Equations (5) and (6), respectively.

(**a**) OImg01

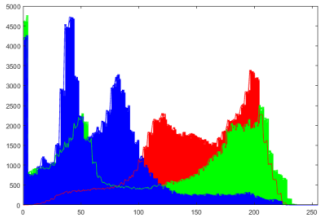
(**b**) OImg02

(**c**) OImg03

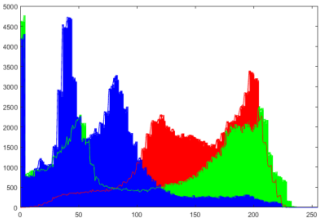
(**d**) EImg01-1

(**e**) EImg02-1

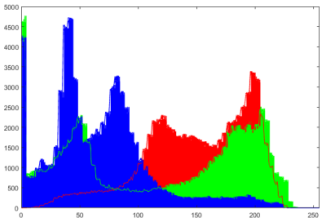
(**f**) EImg03-1



(**g**)



(**h**)

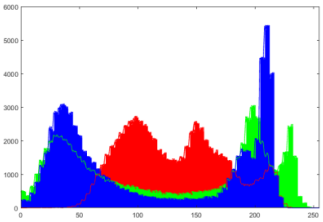


(**i**)

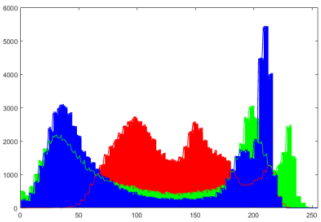
(**j**) EImg01-2

(**k**) EImg02-2

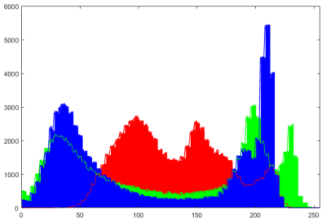
(**l**) EImg03-2



(**m**)



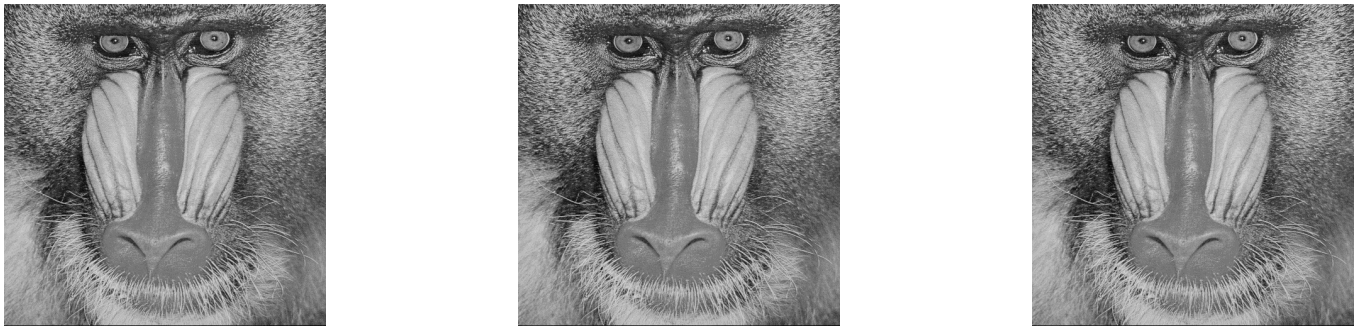
(**n**)



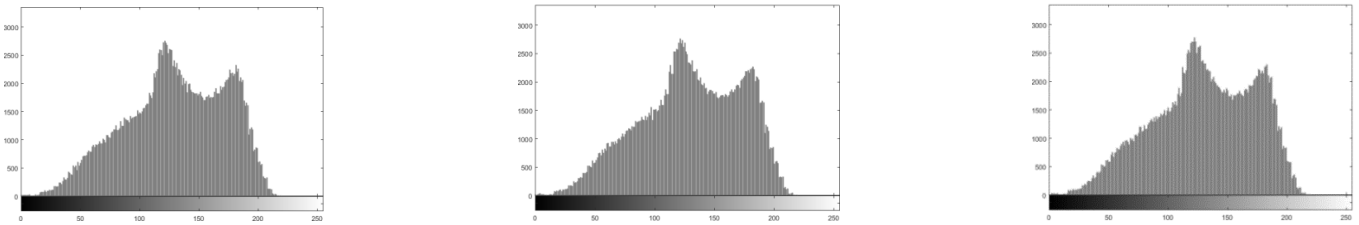
(**o**)

Figure 5. Outcomes of simulation tests for pairings of original and reference colour images in the dataset presented earlier in Figures 3 and 4. The original images are presented in the first row (**a**–**c**), while their encrypted versions with the Peppers (RImg01) image as reference image are presented in the second row (**d**–**f**). Third row (**g**–**i**), presents histograms of the encrypted versions of these images. Similarly, the fourth row (**j**–**l**) presents encrypted versions of the original images with Lake (RIm02) image as reference image, and their respective histograms are presented in the last row (**m**–**o**).

(**a**) OImg04 (**b**) OImg05 (**c**) OImg06

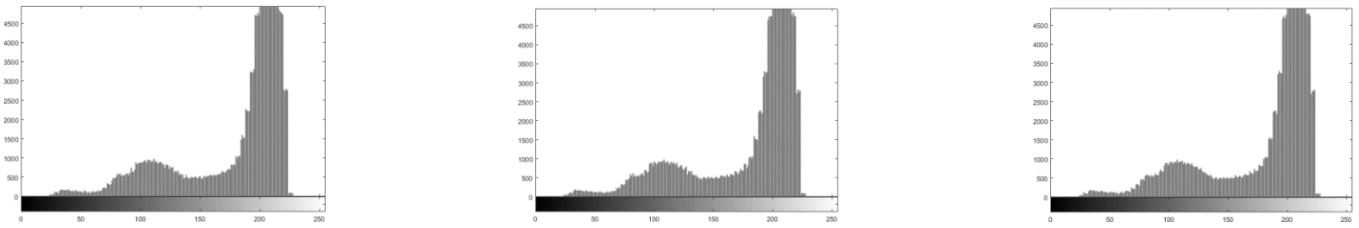


(**d**) EImg04-3 (**e**) EImg05-3 (**f**) EImg06-3



(**g**) (**h**) (**i**)

(**j**) EImg04-4 (**k**) EImg05-4 (**l**) EImg06-4



(**m**) (**n**) (**o**)

Figure 6. Outcomes of simulation tests for pairings of original and reference greyscale images in the dataset presented earlier in Figures 3 and 4. The original images are presented in the first row (**a**–**c**), while their encrypted versions with the Baboon (RImg03) image as reference image are presented in the second row (**d**–**f**). Third row (**g**–**i**) presents histograms of the encrypted versions of these images. Similarly, the fourth row (**j**–**l**) presents encrypted versions of the original images with Plane (RIm04) image as reference image, and their respective histograms are presented in the last row (**m**–**o**).

$$PSNR(R,E) = 20\log_{10}\left(\frac{MAX_R \times \sqrt{x \times y}}{\sqrt{\sum_{i=0}^{x-1}\sum_{j=0}^{y-1}[R(i,j)-E(i,j)]^2}}\right) \quad (5)$$

$$SSIM(R,E) = \frac{(2\mu_R\mu_E + T_1)(2\sigma_{R,E} + T_2)}{(\mu_R^2 + \mu_E^2 + T_1)(\sigma_R^2 + \sigma_E^2 + T_2)} \quad (6)$$

where MAX_R points to the maximum pixel value of the reference image R, T_1 and T_2 are constants, μ and σ are the mean and variance, respectively, while E specifies the encrypted image relative to an $x \times y$-dimensional reference image R. Generally, higher PSNR values indicate good visual quality often at levels imperceptible to the human visual system (HVS). Tables 1 and 2 present outcomes of the visual quality tests for our proposed scheme in terms of the PSNR (Table 1) and SSIM (Table 2) quality metrics. Defined within a range [0,1], values of SSIM closer to 1 indicate high visual quality of the encrypted image.

Table 1. Outcomes of PSNR (in dB) test for encrypted images.

Reference Image	Original Image					
	OImg01	**OImg02**	**OImg03**	**OImg04**	**OImg05**	**OImg06**
RImg01	43.4264	43.4192	43.4203	-	-	-
RImg02	43.9165	43.9033	43.8933	-	-	-
RImg03	-	-	-	43.2824	43.2937	43.2813
RImg04	-	-	-	43.2486	43.2509	43.2394

Table 2. Outcomes of SSIM test for encrypted images.

Reference Image	Original Image					
	OImg01	**OImg02**	**OImg03**	**OImg04**	**OImg05**	**OImg06**
RImg01	0.9858	0.9857	0.9856	-	-	-
RImg02	0.9824	0.9825	0.9823	-	-	-
RImg03	-	-	-	0.9981	0.9980	0.9981
RImg04	-	-	-	0.9573	0.9580	0.9577

5.2. Efficiency Tests

To assess the efficiency of our proposed schemes, we report outcomes three analyses (histogram, correlation, and entropy) to ascertain how well the scheme blends the original and reference images for secure visually meaningful transmission and sharing.

5.2.1. Histogram Analysis

Histogram test is a significant test for evaluating the efficiency of any encryption algorithm as reflected by the frequency distribution of pixel values for the image [29]. Any practical encryption protocol should exhibit identical histograms for different cipher images. Histograms for the original and encrypted images realised using the scheme are presented in Figures 5 and 6, from which we note that all images encrypted using the same reference image manifest identical histograms. Additionally, the histograms for original image (OImg01) and their encrypted versions before embedding onto the reference Baboon image are presented in Figure 7, while those for the original greyscale embedded onto the plane reference image are presented in Figure 8. We note that, prior to embedding onto the reference images, all the encrypted images exhibit identical histograms. Consequently, it can be deduced the the proposed visually meaningful image encryption approach could withstand histogram attacks.

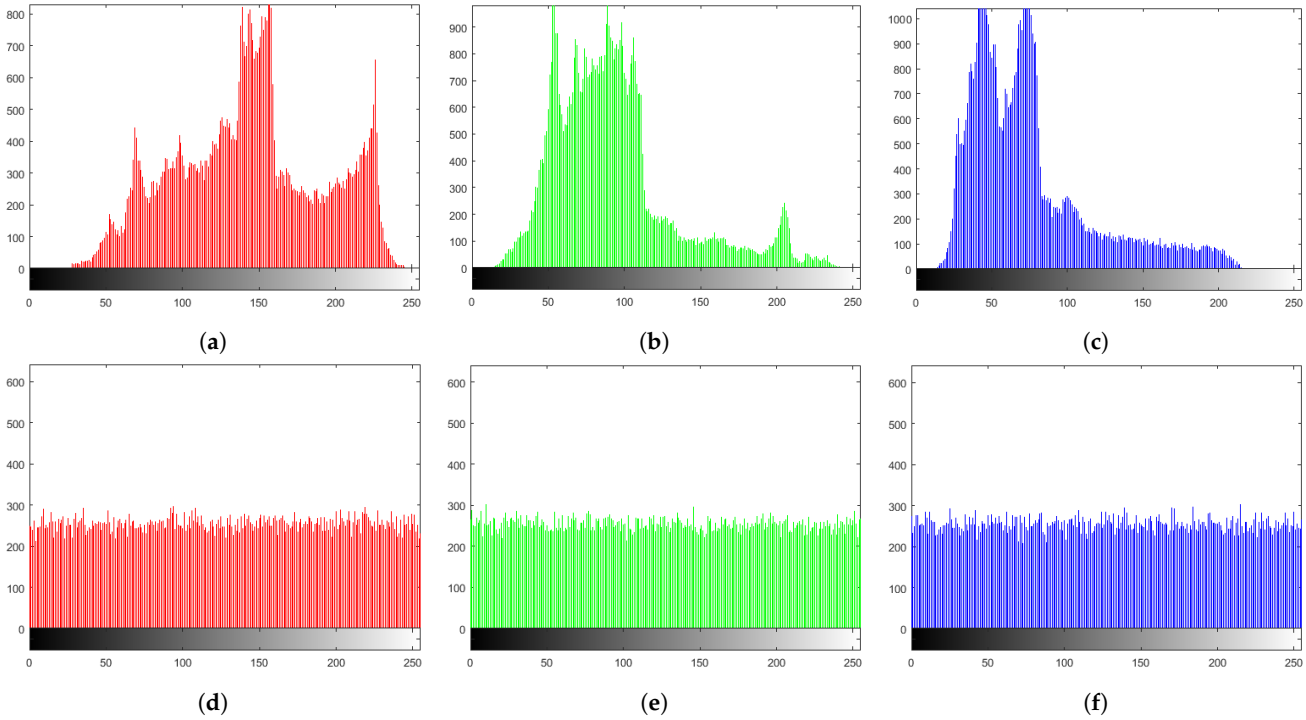


Figure 7. Histograms (**a**–**f**) for OImg01 and its encrypted version before embedding onto the reference.

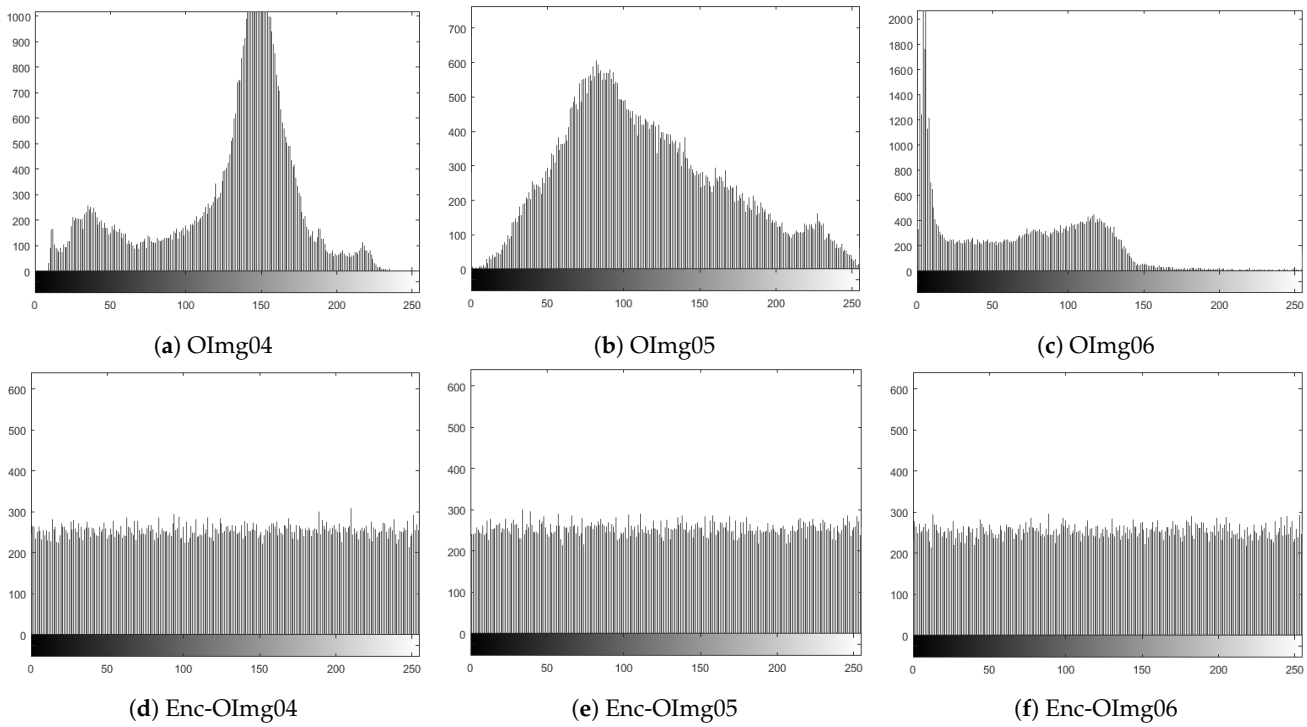


Figure 8. Histograms (**a**–**f**) for grayscale images and their encrypted version before embedding onto the reference.

5.2.2. Correlation Analysis

To measure the concordance between neighbouring pixels in an encrypted image, the measure of correlation coefficient between adjacent pixels is used [25]. Outcomes of correlation coefficients closer to 1 indicate that the image is meaningful. To evaluate the correlation coefficients per channel in the visually encrypted images, 10^4 pairs of neighbouring pixels are selected randomly and computed using Equation (7).

$$Cf = \frac{\sum_{x=1}^{Q}(m_x - \bar{m})(n_x - \bar{n})}{\sqrt{\sum_{x=1}^{Q}(m_x - \bar{m})^2 \sum_{x=1}^{Q}(n_x - \bar{n})^2}} \tag{7}$$

where Q denotes the full number of adjacent pixel pairs in each direction and m_x, n_x are denote to the values of pair neighbouring pixels. Outcomes of Cf measure for images encrypted using our scheme are presented in Table 3 while the correlation distribution for encrypted image EImg01-1 is presented in Figure 9. Both outcomes corroborate claims regarding the meaningfulness of the encrypted images. Similarly, outcomes of the correlation analysis for pairings between the original images and their encrypted versions prior to embedding onto the reference image are presented in Table 4 and the correlation distribution for encrypted image OImg04 is presented in Figure 10.

The two outcomes demonstrate that no intelligible information about the original image can be deduced, which confirms the correlation strength and efficiency of our proposed encryption scheme.

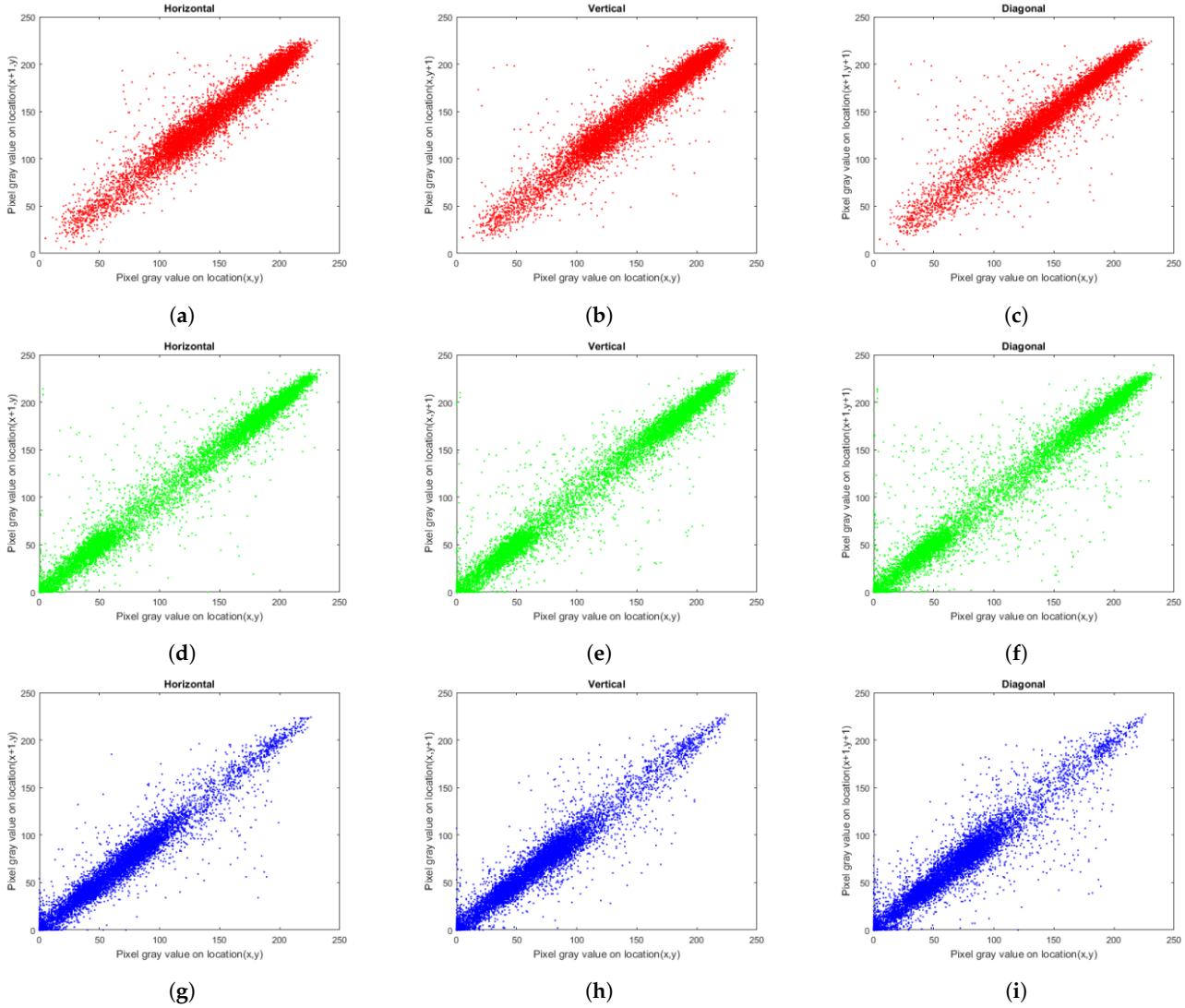


Figure 9. Correlation distribution (**a**–**i**) for encrypted image EImg01-1.

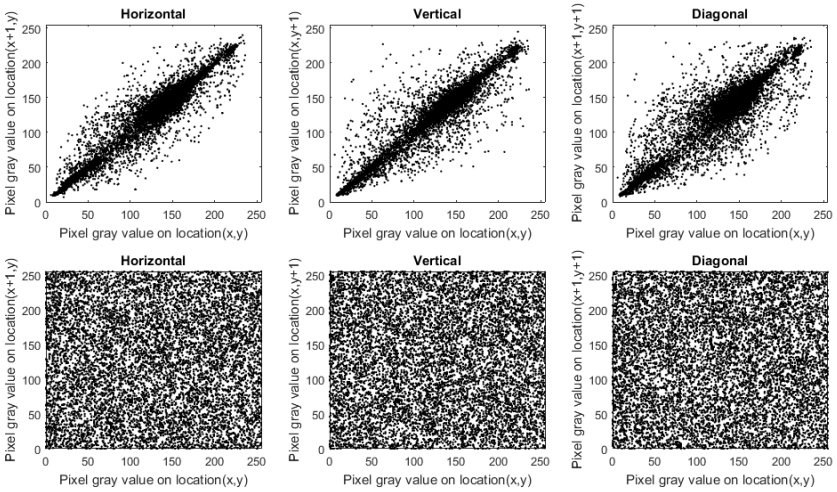


Figure 10. Correlation distribution for OImg04 and its encrypted version before embedding onto the reference image.

Table 3. Correlation coefficients for visually encrypted images.

Encrypted Image	Colour Channel	Direction		
		Horizontal	Vertical	Diagonal
EImg01-1	Red	0.9678	0.9636	0.9600
	Green	0.9844	0.9821	0.9729
	Blue	0.9684	0.9643	0.9507
EImg02-1	Red	0.9676	0.9672	0.9597
	Green	0.9833	0.9815	0.9706
	Blue	0.9688	0.9667	0.9516
EImg03-1	Red	0.9640	0.9665	0.9572
	Green	0.9823	0.9836	0.9726
	Blue	0.9703	0.9650	0.9530
EImg01-2	Red	0.9548	0.9555	0.9451
	Green	0.9664	0.9711	0.9521
	Blue	0.9701	0.9725	0.9553
EImg02-2	Red	0.9553	0.9552	0.9431
	Green	0.9651	0.9731	0.9539
	Blue	0.9705	0.9708	0.9555
EImg03-2	Red	0.9528	0.9568	0.9436
	Green	0.9676	0.9711	0.9548
	Blue	0.9709	0.9708	0.9546
EImg04-3	Grey	0.7756	0.8681	0.7387
EImg05-3	Grey	0.7542	0.8603	0.7288
EImg06-3	Grey	0.7719	0.8629	0.7312
EImg04-4	Grey	0.9662	0.9680	0.9443
EImg05-4	Grey	0.9648	0.9708	0.9414
EImg06-4	Grey	0.9639	0.9683	0.9434

Table 4. Correlation coefficients for pristine images and their encrypted ones before embedding onto a reference image.

Image	Colour Channel	Direction		
		Horizontal	**Vertical**	**Diagonal**
OImg01	Red	0.9126	0.8716	0.8457
	Green	0.9005	0.8433	0.8152
	Blue	0.9182	0.8637	0.8222
Enc OImg01	Red	0.0013	−0.0003	0.0006
	Green	−0.0003	0.0003	−0.0008
	Blue	0.0009	−0.0003	0.0007
OImg02	Red	0.9539	0.9517	0.9165
	Green	0.9645	0.9614	0.9385
	Blue	0.9661	0.9613	0.9414
Enc OImg02	Red	0.0002	−0.0009	−0.0003
	Green	−0.0009	0.0007	−0.0002
	Blue	0.0006	−0.0001	−0.0004
OImg03	Red	0.9343	0.9666	0.9093
	Green	0.9561	0.9801	0.9423
	Blue	0.9751	0.9819	0.9619
Enc OImg03	Red	−0.0008	0.0006	−0.0009
	Green	0.0007	−0.0003	−0.0004
	Blue	−0.0001	0.0006	−0.0007
OImg04	Grey	0.9464	0.9239	0.8796
Enc OImg04	Grey	0.0007	−0.0006	0.0003
OImg05	Grey	0.9162	0.9404	0.8816
Enc OImg05	Grey	−0.0008	−0.0001	0.0001
OImg06	Grey	0.9592	0.9574	0.9143
Enc OImg06	Grey	−0.0004	0.0001	−0.0013

5.2.3. Entropy Analysis

Information entropy is used as a tool to assess the concentration of pixel values per bit-level in an image. For greyscale images, entropy values closer to 8 indicate the efficiency of an encryption technique [30]. Table 5 presents the entropy values for our reference and visual encrypted images. Similarly, Table 6 reports the entropy values for pairings of our original images and their encrypted versions prior to their embedding onto the reference images.

As targeted, both tables record entropy values close to an optional value of 8, which is further testimony of the efficiency of our proposed encryption scheme.

Table 5. Information entropy for reference and visual encrypted images.

Image	Information Entropy
RImg01	7.6698
EImg01-1	7.7253
EImg02-1	7.7252
EImg03-1	7.7252
RImg02	7.7621
EImg01-2	7.7711
EImg02-2	7.7710
EImg03-2	7.7711
RImg03	7.3578
EImg04-3	7.3591
EImg05-3	7.3590
EImg06-3	7.3591
RImg04	6.6776
EImg04-4	6.6895
EImg05-4	6.6894
EImg06-4	6.6896

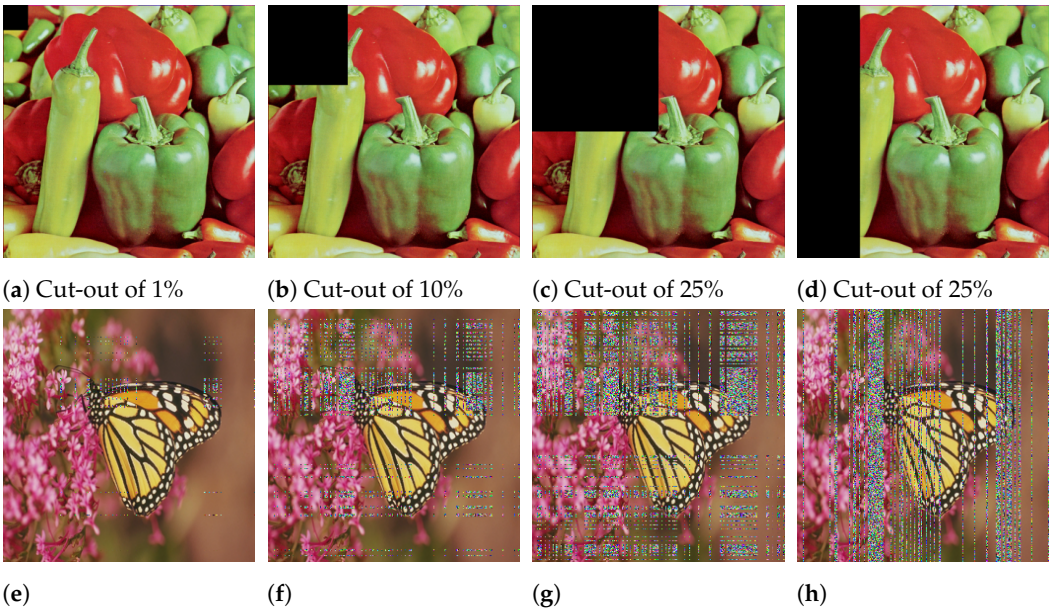
Table 6. Information entropy for original images and their encrypted versions before embedding them onto the reference images.

Image	Original	Encrypted
OImg01	7.5225	7.99909
OImg02	7.6658	7.99906
OImg03	7.0686	7.99915
OImg04	7.1586	7.99748
OImg05	7.6684	7.99728
OImg06	6.5233	7.99726

5.3. Robustness Tests: Occlusion and Data Loss Attacks

In real-world smart systems and similar applications, encrypted images are transmitted via noisy channels, which makes them susceptible to tampering, loss, and other violations. To appraise the robustness of our encryption mechanism and its ability to withstand data loss due noise addition, we considered the addition of various levels in Salt and Pepper (S&P) noise onto the encrypted images and using our decryption procedure, we evaluated for attempts to recover the original images from the violated versions.

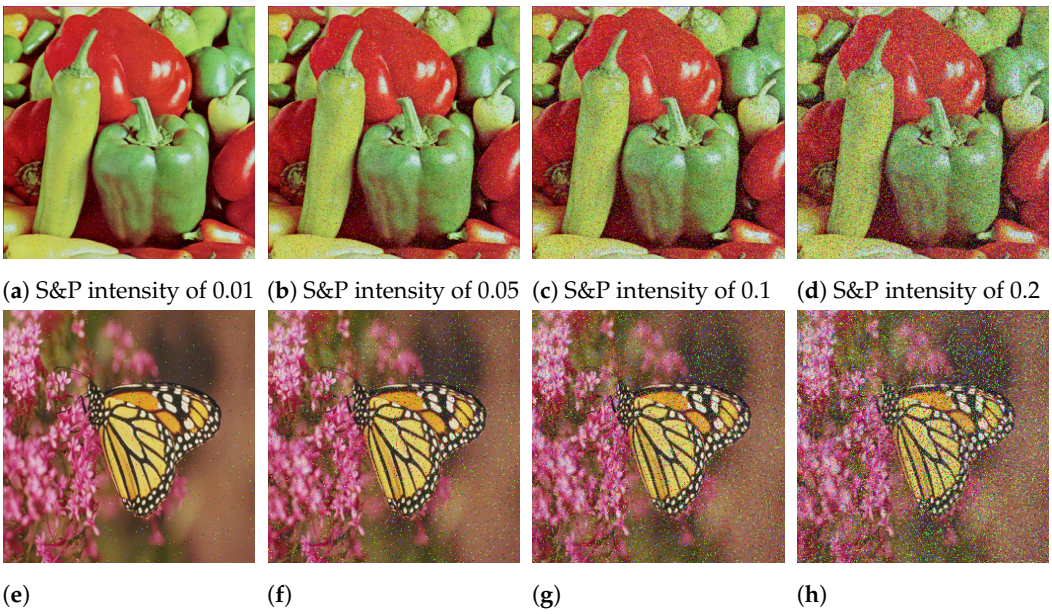
For the occlusion attacks, we considered using cut-outs of varied sizes to occlude parts of the encrypted images. Figures 11 and 12 present outcomes of the occlusion and noise attacks. The good visual quality from both outcomes manifests the robustness of our proposed encryption scheme to occlusion and noise addition attacks.



(**a**) Cut-out of 1% (**b**) Cut-out of 10% (**c**) Cut-out of 25% (**d**) Cut-out of 25%

(**e**) (**f**) (**g**) (**h**)

Figure 11. Outcomes of occlusion attacks (**e**–**h**) with various cut-outs of parts from the encrypted image EImg01-1 (**a**–**d**).



(**a**) S&P intensity of 0.01 (**b**) S&P intensity of 0.05 (**c**) S&P intensity of 0.1 (**d**) S&P intensity of 0.2

(**e**) (**f**) (**g**) (**h**)

Figure 12. Outcomes of noise attacks (**e**–**h**) with various Salt and Pepper (S&P) noise intensities (**a**–**d**) appended to the encrypted image EImg01-1.

5.4. Key Sensitivity Test

Key sensitivity is an important test for the security of any cryptographic approach. It is a measure of the sensitivity of key parameters to the influence or circumvent the decryption process. To appraise the key sensitivity of our proposed scheme, we varied tiny parts of the secret key and evaluated if the protected original images could be violated. Outcomes of these tests for the indicated variations in the secret key are reported in Figure 13. Quantitatively, we employed the Number of Pixel Change Rate (NPCR) metric, which is expressed in Equation (8), to assess the key sensitivity of the proposed scheme.

$$\begin{aligned} NPCR(OIm, DIm) &= \frac{\sum_{x,y} f(i,j)}{M} \times 100\%, \\ f(i,j) &= \begin{cases} 1, & if\ OIm(i,j) \neq DIm(i,j) \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{8}$$

where *OIm* and *DIm* denote the pristine and decrypted images, and *M* denotes the total pixels in the image. NPCR values for the original image OImg01 are presented in Table 7 while, as noted earlier, the outcomes for different alternations to the secret decryption key are presented in Figure 13.

Both outcomes confirm the proposed schemes sensitivity to tiny modifications to its secret key as the image recovery is unsuccessful in all attempts reported (as seen in Figure 13).

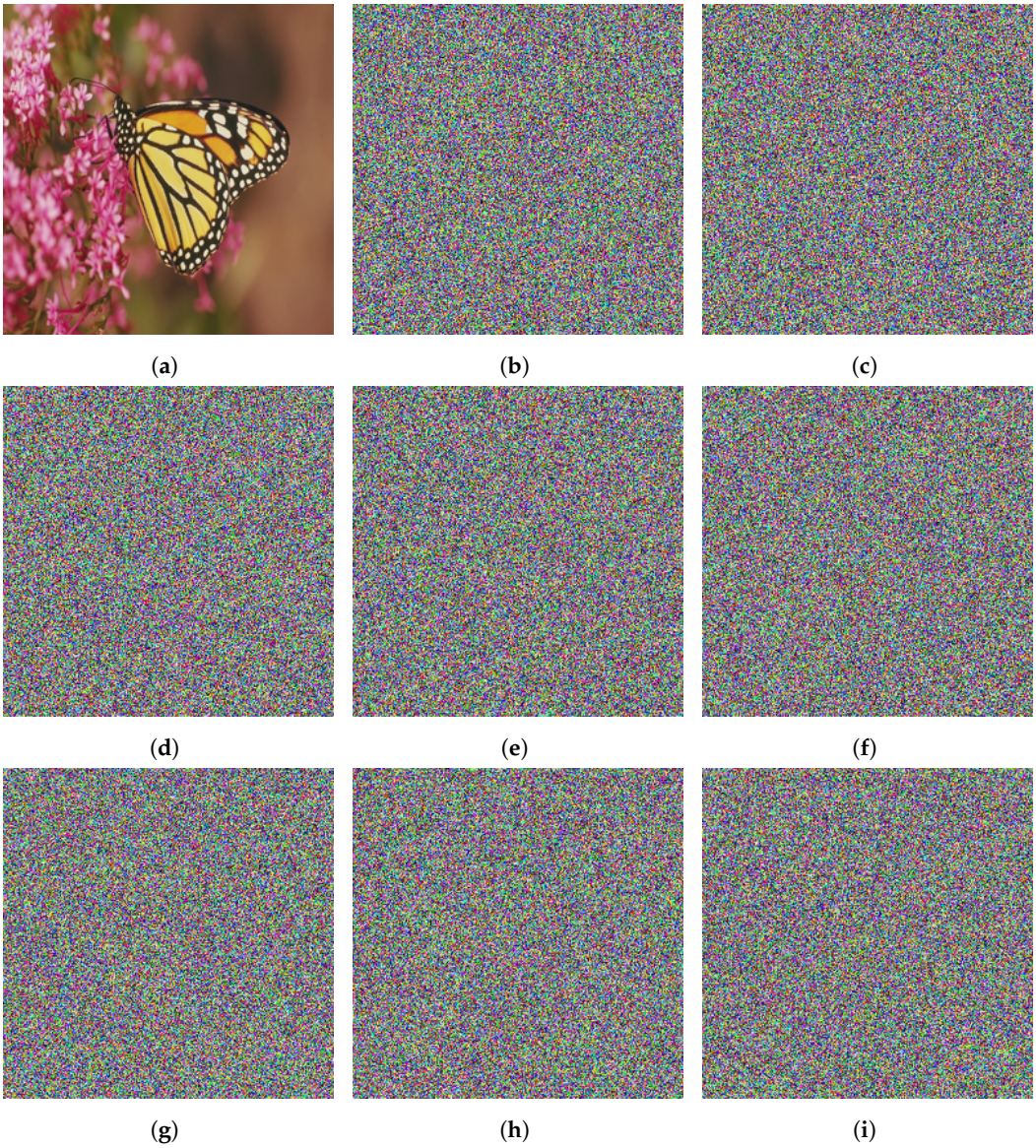


Figure 13. Outcomes of decryption process for the encrypted image EImg01-1 using different values of key parameters. (**a**) Correct key. (**b**) Correct key except for N = 263. (**c**) Correct key except for S = 520. (**d**) Correct key except for $\beta = \pi/3$. (**e**) Correct key except for $\theta_0 = \pi/2$. (**f**) Correct key except for $\theta_1 = \pi/2$. (**g**) Correct key except for $\theta_2 = \pi/6$. (**h**) Correct key except changing the first bit of T from 0 to 1. (**i**) Correct key except removing the last bit of T.

Table 7. NPCR values for the original image OImg01 and the results illustrated in Figure 13.

Image Pairing	NPCR (%)
Figures 3a and 13a	0
Figures 3a and 13b	99.6027
Figures 3a and 13c	99.6098
Figures 3a and 13d	99.5890
Figures 3a and 13e	99.6078
Figures 3a and 13f	99.6047
Figures 3a and 13g	99.6139
Figures 3a and 13h	99.6241
Figures 3a and 13i	99.6043

5.5. Performance Analysis

To establish the efficiency of our proposed scheme, in this section we compare its performance in terms of visual quality metrics alongside recent and similar image encryption techniques. Using outcomes reported earlier for PSNR (Table 1) and SSIM (Table 2), the performance analysis in Table 8 compares the recorded outcomes alongside those from [13–16,22].

As presented in the table, our proposed scheme performs better than most of the competing techniques in the range of 15 to 44% and up to 29.5% for the PSNR and SSIM image quality metrics.

Table 8. Comparison of the average PSNR and SSIM value for our algorithm besides other related algorithms.

Cryptosystem	PSNR(dB)	SSIM
Proposed	43.4646	0.9810
[13]	35.2058	0.9584
[14]	32.0502	0.9937
[15]	24.0488	0.6913
[16]	30.9728	0.8554
[22]	36.9028	0.9987

6. Concluding Remarks

A confluence of efforts geared towards deployment of technologies on smart systems on the one hand and the invigorated interest in and accelerated march towards the quantum computing era on the other indicate not only the ubiquity, but also the vulnerability of images that we use in our everyday lives. Considering the need to safeguard the integrity and confidentiality of these diverse types of images, our study proposes an encryption scheme that exploits the potency of quantum walks to substitute the pristine images and then permutate and subsequently embed the substituted images onto a reference image. Not only does our proposed scheme provide tamperproof security for today's computing frameworks, but it also offers safeguards to protect future smart systems that will built using quantum computing hardware. Outcomes from stimulation-based experiments reported in the study highlights the efficiency of the proposed scheme in terms of visual quality, correlation analysis, key space sensitivity and robustness. Additionally, comparisons in terms of visual quality tests indicate that the proposed scheme outperforms recent and similar schemes by as high as 44% and 29.5% for the PSNR and SSIM image

quality metrics. The study and its outcomes suggest potential applications for the proposed scheme in safeguarding smart systems.

Author Contributions: Data curation, A.A.A.E.-L.; Formal analysis, A.A.A.E.-L. and B.A.-E.-A.; Investigation, A.A.A.E.-L. and A.M.I.; Methodology, A.A.A.E.-L., A.M.I. and B.A.-E.-A.; Project administration, A.M.I.; Software, A.A.A.E.-L. and B.A.-E.-A.; Supervision, A.M.I.; Validation, A.M.I. and B.A.-E.-A.; Writing—original draft, A.A.A.E.-L. and A.M.I.; Writing—review & editing, A.A.A.E.-L., A.M.I. and B.A.-E.-A. All authors have read and agreed to the published version of the manuscript.

Funding: This study is sponsored in full by the Prince Sattam Bin Abdulaziz University, Saudi Arabia via the Deanship for Scientific Research funding for the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group Project number 2020/01/12173.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cui, L.; Xie, G.; Qu, Y.; Gao, L.; Yang, Y. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* **2018**, *6*, 46134–46145. [CrossRef]
2. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
3. Abd EL-Latif, A.A.; Abd-El-Atty, B.; Abou-Nassar, E.M.; Venegas-Andraca, S.E. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Opt. Laser Technol.* **2020**, *124*, 105942. [CrossRef]
4. El-Latif, A.A.A.; Abd-El-Atty, B.; Amin, M.; Iliyasu, A.M. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **2020**, *10*, 1930. [CrossRef]
5. Benrhouma, O.; Hermassi, H.; Abd El-Latif, A.A.; Belghith, S. Chaotic watermark for blind forgery detection in images. *Multimed. Tools Appl.* **2016**, *75*, 8695–8718. [CrossRef]
6. Nestor, T.; De Dieu, N.J.; Jacques, K.; Yves, E.J.; Iliyasu, A.M.; El-Latif, A.; Ahmed, A. A multidimensional hyperjerk oscillator: dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem. *Sensors* **2020**, *20*, 83. [CrossRef] [PubMed]
7. Amin, M.; Abd El-Latif, A.A. Efficient modified RC5 based on chaos adapted to image encryption. *J. Electron. Imaging* **2010**, *19*, 013012. [CrossRef]
8. Ping, P.; Fu, J.; Mao, Y.; Xu, F.; Gao, J. Meaningful Encryption: Generating Visually Meaningful Encrypted Images by Compressive Sensing and Reversible Color Transformation. *IEEE Access* **2019**, *7*, 170168–170184. [CrossRef]
9. Yan, X.; Wang, S.; Abd El-Latif, A.A.; Niu, X. Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. *Multimed. Tools Appl.* **2015**, *74*, 3231–3252. [CrossRef]
10. Abd El-Latif, A.A.; Yan, X.; Li, L.; Wang, N.; Peng, J.L.; Niu, X. A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption. *Opt. Laser Technol.* **2013**, *54*, 389–400. [CrossRef]
11. Armijo-Correa, J.; Murguía, J.; Mejía-Carlos, M.; Arce-Guevara, V.; Aboytes-González, J. An improved visually meaningful encrypted image scheme. *Opt. Laser Technol.* **2020**, *127*, 106165. [CrossRef]
12. Bao, L.; Zhou, Y. Image encryption: Generating visually meaningful encrypted images. *Inf. Sci.* **2015**, *324*, 197–207. [CrossRef]
13. Wang, H.; Xiao, D.; Li, M.; Xiang, Y.; Li, X. A visually secure image encryption scheme based on parallel compressive sensing. *Signal Process.* **2019**, *155*, 218–232. [CrossRef]
14. Zhu, L.; Song, H.; Zhang, X.; Yan, M.; Zhang, T.; Wang, X.; Xu, J. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. *Signal Process.* **2020**, *175*, 107629. [CrossRef]
15. Chai, X.; Gan, Z.; Chen, Y.; Zhang, Y. A visually secure image encryption scheme based on compressive sensing. *Signal Process.* **2017**, *134*, 35–51. [CrossRef]
16. Musanna, F.; Kumar, S. Generating visually coherent encrypted images with reversible data hiding in wavelet domain by fusing chaos and pairing function. *Comput. Commun.* **2020**, *162*, 12–30. [CrossRef]
17. Chai, X.; Wu, H.; Gan, Z.; Han, D.; Zhang, Y.; Chen, Y. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. *Inf. Sci.* **2021**, *556*, 305–340. [CrossRef]
18. Bai, S.; Zhou, L.; Yan, M.; Ji, X.; Tao, X. Image Cryptosystem for Visually Meaningful Encryption Based on Fractal Graph Generating. *IETE Tech. Rev.* **2020**, *38*, 130–141. [CrossRef]
19. Yang, Y.G.; Zou, L.; Zhou, Y.H.; Shi, W.M. Visually meaningful encryption for color images by using Qi hyper-chaotic system and singular value decomposition in YCbCr color space. *Optik* **2020**, *213*, 164422. [CrossRef]

20. EL-Latif, A.A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E.; Mazurczyk, W. Efficient quantum-based security protocols for information sharing and data protection in 5G networks. *Future Gener. Comput. Syst.* **2019**, *100*, 893–906. [CrossRef]
21. Abd-El-Atty, B.; El-Latif, A.A.A.; Venegas-Andraca, S.E. An encryption protocol for NEQR images based on one-particle quantum walks on a circle. *Quantum Inf. Process.* **2019**, *18*. [CrossRef]
22. Su, Y.; Wang, X. A robust visual image encryption scheme based on controlled quantum walks. *Phys. A Stat. Mech. Appl.* **2022**, 587, 126529. [CrossRef]
23. Stergiou, C.; Psannis, K.E.; Gupta, B.B.; Ishibashi, Y. Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. *Sustain. Comput. Informatics Syst.* **2018**, *19*, 174–184. [CrossRef]
24. El-Latif, A.A.A.; Abd-El-Atty, B.; Elseuofi, S.; Khalifa, H.S.; Alghamdi, A.S.; Polat, K.; Amin, M. Secret images transfer in cloud system based on investigating quantum walks in steganography approaches. *Phys. A Stat. Mech. Appl.* **2020**, *541*, 123687. [CrossRef]
25. Abd-El-Atty, B.; Iliyasu, A.M.; Alaskar, H.; El-Latif, A.; Ahmed, A. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. *Sensors* **2020**, *20*, 3108. [CrossRef] [PubMed]
26. SIPI Image Database-Misc. Available online: https://sipi.usc.edu/database/database.php?volume=misc (accessed on 15 October 2021).
27. LIVE Image Quality Assessment Database. Available online: https://qualinet.github.io/databases/image/live_image_quality_assessment_database/ (accessed on 15 October 2021).
28. MedPix. Available online: https://medpix.nlm.nih.gov/home (accessed on 15 October 2021).
29. Abd-El-Atty, B.; Iliyasu, A.M.; El-Latif, A.; Ahmed, A. A Multi-Image Cryptosystem Using Quantum Walks and Chebyshev Map. *Complexity* **2021**, *2021*, 9424469. [CrossRef]
30. Li, L.; Abd-El-Atty, B.; Abd El-Latif, A.A.; Ghoneim, A. Quantum color image encryption based on multiple discrete chaotic systems. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; pp. 555–559.