

A proposed model for text and image encryption using different techniques

Shihab A. Shawkat¹, Israa Al-Barazanchi^{2,3}

¹Department of Quality Assurance and Academic Performance, University of Samarra, Samarra, Iraq

²Baghdad College of Economic Sciences University, Baghdad, Iraq

³College of Computer Science and Information Technology, Universiti Tenaga Nasional (UNITEN), Selangor, Malaysia

Article Info

Article history:

Received Feb 15, 2022

Revised Jun 20, 2022

Accepted Jun 28, 2022

Keywords:

DCT techniques fourth

Information security second

Encryption

MSE

PSNR

RSA3k

XOR

ABSTRACT

Data security and protection is one of the most common technologies used in the field of computer science. This is because of its great importance in all fields related to daily life, whether political, economic, and other aspects change. In this research paper, a new intelligent system that concentrates on image and text encryption and decryption is proposed. Furthermore, the image recognition rate is increased. In this paper, the Rivest Shamir Adleman 3 key (RSA3k) algorithm is used but in a new technique to encrypt and decrypt text. The proposed technique relies on using square root of public key as private key. XOR operation for colored images encryption and decryption is performed. By calculating signal to noise ratio (PSNR), mean square error (MSE), and bit error rate (BER), the most important things that we address how to provide data security for large data based on encryption techniques and increase the security of multimedia data and texture data and address the problem of time and accuracy in image matching. The results show that the quality of images after decryption is good.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Shihab A. Shawkat

Department of Quality Assurance and Academic Performance, University of Samarra

Samarra, Iraq

Email: shahab84ahmed@gmail.com

1. INTRODUCTION

The data security is one of the most important challenges facing the human since different eras because of their relationship and close to a lot of important things in the life of rights, such as the security of nations, preserving the lives of people from terrorist attacks, as a significant impact on trading, economic [1]. Therefore, there're interested researchers in this area and especially after the increase in piracy and spy on information, where many of the academic research conducted in this area operations. The difficulty of finding a complete definition or full definition of artificial intelligence but not defined in the following that it is the study of ideas in a way that enables the computer to deal in a smart [2], [3]. Data encryption is a way of protecting the data that's based on artificial intelligence. The encryption is necessary in the internet applications of the image as it is the use of encryption to protect the images or data in transit across networks such as (network internet and mobile phones and wireless communication systems and Bluetooth devices) [4]. Because of its ability to compressed steam, the discrete cosine transform (DCT) technique is considered one of the most common techniques used in a wide variety of image detection and advanced forecasting applications. In some variables, it condenses most of the data transmission [5]. The sparse representation (SR) being a powerful and very important tool for acquiring and compressing high-dimensional signals, and this success for the sparse representation originally due to the fact the important categories of brands such as images and sound [6]. Rivest Shamir Adleman (RSA) encryption algorithm is the way of the use of certain

keys where the information is encrypted in a manner that is understandable when viewed by unauthorized people to look at it when they penetrate the system [7]. This paper introduces a new technique that uses the combination of sparse and DCT to enhance recognition rate. It also proves that XOR operation can be used on colored image encrypt and decryption and show the use of RSA 3 key (RSA3k) algorithm on text encryption and decryption based on square root operation. Section 2 outlines prior work for encryption/decryption algorithms, section 3 presents the proposed method, section 4 the output and evaluation, section 5 the experimental findings, and section 6 the conclusion and potential research.

2. PREVIOUS WORKS

Most previous works of the have hidden a particular text or image based on chaotic systems to generate random chains determine the map of the spread of secret data was used. Facial detection using separate covariance translate pouch (DCT) detects global and regional forms on the anterior margin of a face images, according to Rezende [8]. Is cropped facial image obtained from the user that is extracted facial image in front of me only, it is divided based on pixel images. Sookhak *et al.* [9] provided an approach in conjunction with RSA algorithms and digital signature. They merged a unique ability to control technology-based access with authentication to mutual basis data security and efficiency in cloud computing. Nag *et al.* [10] adopted a hybrid cryptography method that encrypts the image processor that use the reverse process after rearranging the pixel values to use the invariant transformation. They use an invariant switch up with four 8-bit keys that reallocate the pixel to various locations. The factors external then is divided into 2 pixels by 2-pixel frames, with each region being encoded with four 8-bit keys using reverse process. The technique requires a 64-bit total key size. The association between adjacent pixels was drastically decreased after the affine transform, according to their findings. Thabit *et al.* [11] proposed methodology included various clouds that will be available for use by the user. But before using cloud computing service user to register, during user registration you will need to choose the encryption algorithm and then the user enters the security key to be used to encrypt the data for this user only. After the end user registration process will get to know different keys that can be used to encrypt/decrypt the data that the user will be stored via cloud. Kumari *et al.* [12] provided a symmetric key image encryption technique based on the first step to change locations every pixel in the image using a bit sub-key 4 and 8 then the coding pixel values by XOR and identification keys 8-bit where XOR process that change the values of each pixel has been tested on various gray scale images 256×256 showed the results well. Seyedzade *et al.* [13] suggested a new encryption technique centered on the SHA-512 hash function. The algorithm is split into two categories: the first performs a data pre-processing process to move half of the picture. The hash value is used in the first to create a randomization block. The masks then are XORed with the picture's other portion, which will be coded. Waschke [14] provide mythology for address the development of design for data encryption as well as we unzip encrypted in a network environment using the RSA algorithm with a given type size. The algorithm allows the sender of a message to employ staple keys to encrypt the message and the recipient is sent a special key that was created using a data base reserved. Key special incorrect still will decode the encrypted message, but in a different way from the original message. Otaibi and Gutub [15] proposed safe image data using a combination of several encryption techniques and permutations, they purposed of their work present security in the pictures, which is the main purposed of the system data increase. The images file encryption and decryption data encryption done in such a way that makes it convenient for users. Barazanchi *et al.* [16] looks at the fundamentals of cryptography and reflects on the evolution of RSA and increasing the sophistication of the secret system to create a more secure in programs. We will focus on the Hash function in this venture by introducing certain flexibility to the 3keys (3k) This implementation would improve the application's safety and sophistication while keeping the encryption and authentication times the same. The study also outlines how cryptography can be used to improve cryptography. Furthermore, the RSA method generates dual protection.

3. THE PROPOSED METHOD

3.1. Image encryption and decryption

3.1.1. DCT and SR

DCT this method is useful in a variety of fields, including physics and technology, as well as extraction of features. Since it is a reliable and versatile face detection technology that uses some apply statistical, it is commonly used in jpeg. Scientists in the disciplines of image recognition, machine learning, neural networks, and problem solving have been drawn to dimension reduction (SR). It also has a clear track record in both theoretical and practical studies [17], [18]. The following equation defines the general equation for a 2D (N by M image) DCT.

$$F(u, v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda_{i=0}^M \Lambda(j) \cdot \cos \left[\frac{\pi \cdot u}{2 \cdot N} (2i + 1) \right] \cos \left[\frac{\pi \cdot v}{2 \cdot M} (2j + 1) \right] \cdot f(i, j) \quad (1)$$

The DCT function in row $k1$ and column $k2$ of the cotter is $F(u, v)$. $F(i, j)$ is the device's strength in row I and column j ; in most pictures, the control output is concentrated at lower energies, which appear inside the DCT's upper left corner. Because the lower right caught up different speeds, analysis is done because they are mostly small - small enough to still be ignored with no apparent noise. The following equation for a signal's local features (SR) in an overcomplete vocabulary. The question of local features is to find a $M1$ vector vector x such that $y = Ax$ and $\|x\|_0$ is minimized [19], i.e. given a $N M$ matrix A comprising the items of an over full vocabulary in its rows, with $M > N$ and typically $M \gg N$, and a signal y RN.

$$x = \min \|x'\|_0 \text{ s.t. } y = Ax \quad (2)$$

Where $\|x\|_0$ is the ℓ_0 norm and is equivalent to the number of non-zero components in the vector x .

3.1.2. XOR operation

There are many logical functions used for encryption technique like “not”, “and”, and “or”. These logical functions sometimes used in stream cipher, so it's offered a solid security in web browser area when it's connected to some server. The logical operation considered the basic for the one-time pad. When the cipher is not suitable, the protection is eroded [20]. Image encryption and decryption the detail process of image encryption and decryption. A new combination of the two main processes of our system are (DCT and sparse representation, XOR operation) representation was proposed in this paper to improve the recognition rate and database searching time and loading time, is shown in the block diagram given in Figure 1.

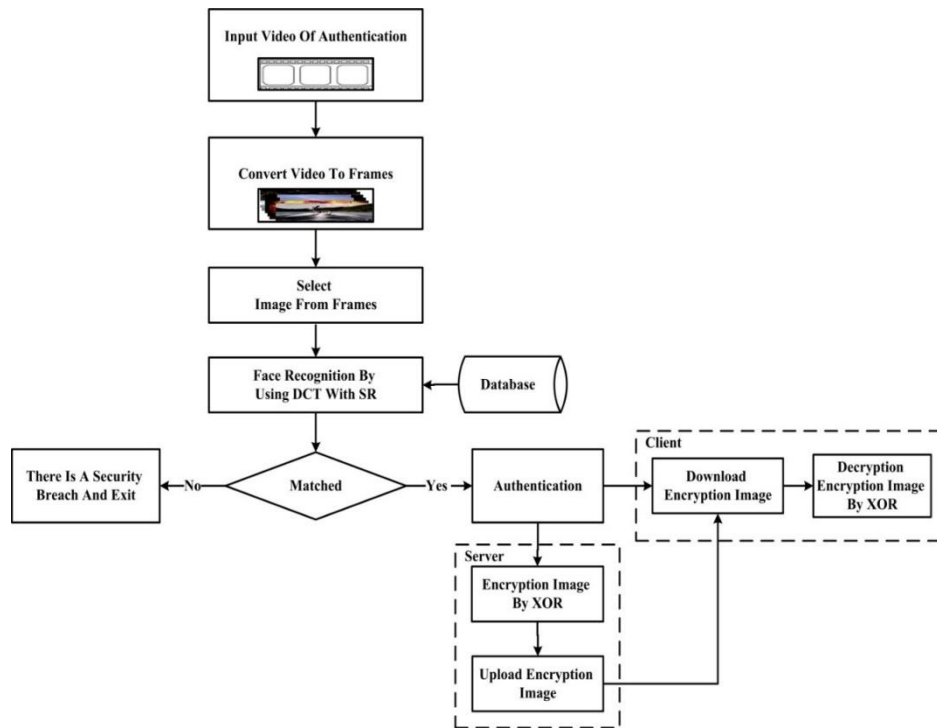


Figure 1. Detailed representation of the proposed scheme of image (encryption and decryption)

In this proposed begin the upload a video, after starting the video, the application uses only sparse representation algorithm to make authentication and recognition and return the time taken in the database searching and loading. The same process is made but using our proposed combination of DCT and sparse algorithms. Then is supposed to where the photo that would be encrypted by using XOR operation. The XOR operation are used to encrypt and decrypt color images, also peak signal-to-noise ratio (PSNR) are used to show the difference between two images, and the mean squared error (MSE) to extract the rate error and bit error rate (BER).

3.2. Text encryption and decryption by RSA3k

The Massachusetts Institute of Technology (MIT) colleagues created RSA as the public-key cryptography and unsymmetrical cypher as the source. For its credibility and detailed investigation, RSA was chosen. Since it is industrial, a block chain model is generally marketed and used in the consumer and corporate interaction sectors. The flexibility of RSA's main size set, which ranges from 2 to 2048 bits, has made it more useful in popular advances. The data lengths preferred by the developer or user determines the application's protection. With this method, a key with such a duration of 1024 bits is being used. Even though 512-bit keys are still often used in apps [21], [22]. Public cryptographic authentication is a term used to describe the authentication of a private key pair. In this group of formulas, a single key is often used to 'encrypt' and 'decipher' the texts. Because of key, every correspondence between complex parties will be kept private. Each orator ought to have a secret identifier to ensure the highest level of protection. As a result, both reporters must ensure that the user key is kept secret [23]. The main generation is the first step in RSA simulations. Furthermore, each user must generate a set of keys [24]. The Hash function can be used for both digital certificates and public key, making it more difficult for those attempting to decode information. RSA employs traditional kinetic arithmetic when working to numbers that have thousands of digits. The following steps generate a transport layer security (TLS) private and common button. Two of the prime numbers are chosen including p , q and r . Modulus by sub 2 can be calculated using these numbers such as $n = p \times q \times 2$.

- As the common integer, the third integer e is chosen, that can multiply evenly. It is highly relevant to the $(p - 1)$, $(q - 1)$, and $(r - 1)$ products.
- The number d is a personal integer that can be derived from the coefficient $\frac{(ed-1)}{(p-1)(q-1)(r-1)}$.
- The keys n and e are a number set. Also, when q and p are large numbers, these measures are ineffective for determining d from e and n .
- For the encryption algorithm M , the cypher text C is generated using a digital signature. $C = Me \text{ Mod } n$ is used for this.
- The recipient decrypts the required cypher text using the secret key and $M = Cd \text{ Mod } n$.

The frame diagram is shown in Figure 2 depicts the detailed method of text encryption and decryption. After the encryption point, this block diagram starts. Our system's key encryption method is RSA3k, as seen in the diagram.

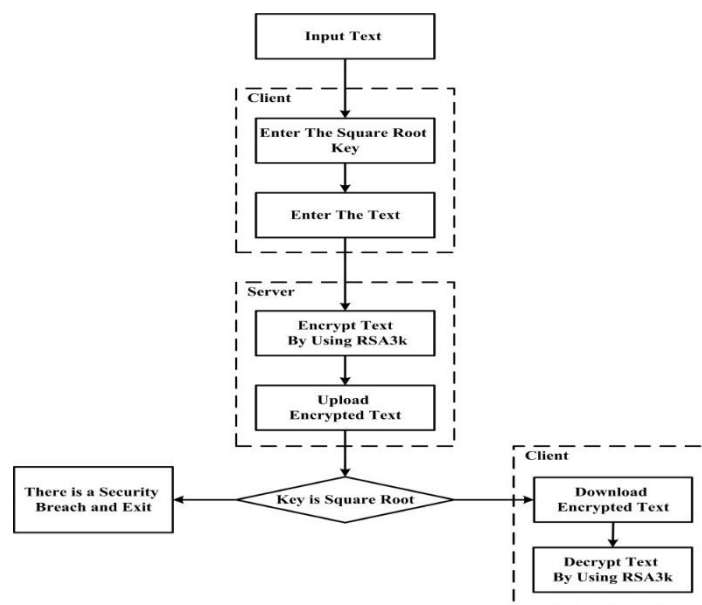


Figure 2. Detailed representation of the proposed scheme of text (encryption and decryption)

After authentication, the user would have two systems a system that makes encryption and decryption for the authenticated image of person and a system that makes encryption and decryption for text. If the user chooses to use the text encryption system. After the encryption process using RSA3k is complete a time of encryption and uploading is computed, and the cipher text is shown to the user using Matlab. Then after that, the asked to enter the private password and when the decryption process using RSA3k is finished a new window is shown to the user using Matlab.

4. THE PERFORMANCE AND EVALUATION

In this section explain the performance and evaluation, the most important things that we address how to provide data security for large data based on encryption techniques and increase the security of multimedia data and texture data and address the problem of time and accuracy in image matching. The results show that the quality of images after decryption is good. The proposed technique implemented using Matlab R2017a software running on a personal computer with a 2.27 GHz Intel (R) Core (TM) i5 CPU, 8 GB RAM and Windows 10 as the operating system. The obtained results and calculated data were evaluated using four: (PSNR, MSE, BER, and recognition rate) statistical parameters as described [25], [26].

4.1. PSNR

PSNR refers to the accuracy of the secret text in compared to the traditional image. It measures the encrypted picture's perceptual quality. To put it another way, it measures and analyses how close two figures are. The greater the PSNR of an encrypted picture, the higher the efficiency of the encrypted picture or the greater the robustness of the cipher text. The PSNR is determined by using the calculation:

$$PSNR = 10 \log_{10} \left[\frac{I^2}{MSE} \right] \quad (3)$$

Where I is the largest achievable value of a pixel in the image (for example, the peak amount for a gray image is 255) and MSE seems to be the sum of squares.

4.2. MSE

The degree of average value between both the main image and the encrypted image is calculated using the MSE function. The discrepancy between both the predicted data of the initial and encrypted images is rounded, and the mean is then measured. When there are a lot of bugs, the RMSE is used. This is due to the fact that it gives these mistakes a bunch of fat. The MSE is calculated as:

$$MSE = \frac{1}{R \times C^2} \sum_{i=0}^n \sum_{j=1}^m (X_{ij} - Y_{ij})^2 \quad (4)$$

X_{ij} is the strength of X_{ij} the pixel in the cover picture, and Y_{ij} seems to be the strength of Y_{ij} the pixel in the steganographic, where R and C are the number of rows or columns in the cover picture, X_{ij} is the strength of X_{ij} the pixel in the cover photo, and Y_{ij} is the frequency of Y_{ij} the segment in the steganography, respectively.

4.3. BER

The quantity obtained in error divided by the number of bits transmitted is known as the data rate (BER). The BER can be calculated by measuring the likelihood of a bit being provided wrongly leading towards sound. The BER is a straightforward term with a straightforward description and calculation.

$$BER = \text{Errors} / \text{Total Number of Bits} \quad (5)$$

4.4. Recognition rate

Is the assessment tool the benchmark by which any facial recognition program's output and success are measured? criteria for evaluating output aim to differentiate, contrast, and analyze a host of variables such as brand depends, position, light, and photographs, as well as how to adjust current performance standards widely used in profile. The Identification Rate is determined as shown in the diagram following.

$$\text{Recognition Rate} = (\text{no. of correctly identified images} / \text{total no. of images}) \times 100 \quad (6)$$

5. EXPERIMENTAL RESULTS

The comparison between a combination of a sparse representation algorithm and DCT and sparse representation algorithm alone using database. A make a comparison between recognition rate and database loading and searching time between two different algorithms. The result will show that combination provide better recognition rate, the user database description consists of: (total number of images: 100, number of images per person: 4, total number of persons: 25).

5.1. Database loading and searching time

In this section will explaining the database loading and searching time, a make a comparison between recognition rate and database loading and searching time between two different algorithms and show how database loading time compression with the result that will show that combination provide better

recognition rate. The following Table 1 illustrates the difference between combination of DCT and SR, and SR alone in database loading time. Which will be in the form of database loads from (block 8×8) to (block 128×128) and that have been worked on successively and the results will show the difference between these loads.

The difference between the combination of DCT and SR, SR alone in database searching time are shown in following Table 2. Which will be in the form of database loads from (block 8×8) to (block 128×128) and that have been worked on successively and the results will show the difference between these loads. It shows that DCT and SR, SR combination decrease database searching time.

Table 1. Database loading time compression

| No. | The blocks | Combination of DCT and SR time load/sec | SR time load/sec | The difference |
|-----|---------------|---|------------------|----------------|
| 1 | Block 8×8 | 2.05973 | 2.18563 | 0.12556 |
| 2 | Block 16×16 | 2.01381 | 2.22272 | 0.20882 |
| 3 | Block 32×32 | 2.04644 | 2.18652 | 0.14011 |
| 4 | Block 64×64 | 2.07657 | 2.21265 | 0.13610 |
| 5 | Block 128×128 | 2.09879 | 2.26488 | 0.11406 |

Table 2. Database searching time

| No. | The blocks | Combination of DCT and SR searching time/sec | SR searching time/sec | The difference |
|-----|---------------|--|-----------------------|----------------|
| 1 | Block 8×8 | 0.014081 | 0.094779 | 0.080711 |
| 2 | Block 16×16 | 0.019696 | 0.079808 | 0.060119 |
| 3 | Block 32×32 | 0.017018 | 0.101817 | 0.084812 |
| 4 | Block 64×64 | 0.028011 | 0.110178 | 0.082171 |
| 5 | Block 128×128 | 0.037005 | 0.131142 | 0.081044 |

5.2. Average of recognition rate

In this section will explaining the average of recognition rate, a make a comparison between recognition rate and database loading and searching time between two different algorithms and show the average of recognition rate comparison (result of 100 images). In Table 3 the average of recognition rate when using (100 images) in the database from (block 8×8) to (block 128×128) using DCT and SR combination is 95.76% while the average of SR only is 92.5%. Used the equation which represent the recognition rate for the faces in the image.

Table 3. Average of recognition rate comparison (result of 100 images)

| No. | The blocks | Average of recognition rate | |
|-----|---------------|-----------------------------|-------|
| | | DCT and SR | SR |
| 1 | Block 8×8 | 98.5% | 94.6% |
| 2 | Block 16×16 | 97.2% | 93.2% |
| 3 | Block 32×32 | 95.5% | 92.8% |
| 4 | Block 64×64 | 94.1% | 91.3% |
| 5 | Block 128×128 | 93.5% | 90.6% |
| 6 | Average | 95.76% | 92.5% |

5.3. Comparing the results against another approaches

In this section will explaining comparing the results against another approaches, a make a comparison between recognition rate and database loading and searching time between two different algorithms and show the comparison with the previous works. To test the effectiveness of the proposed algorithm, the following performance criteria are used: accuracy, time/sec. Table 4 shows the proposed algorithm results comparison between with the previous works in general, as show in Table 4. The database loading has been and as a result the searching time has been reduced moreover, the recognition rate has been increased. In future work we will try to combine another algorithm with the presented system to improve the results providing higher security and quality as compared to existing techniques.




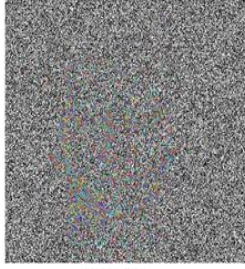





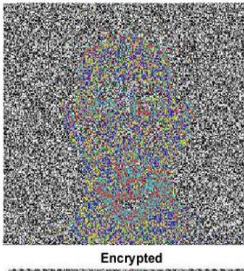


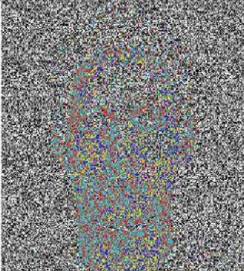

Table 4. The comparison with the previous works

| No. | Model | Accuracy | Time/sec |
|-----|---------------------------------|----------|----------|
| 1 | Wang and Xu [27] | Medium | Medium |
| 2 | Dabbaghchian <i>et al.</i> [28] | High | Medium |
| 3 | Chadha <i>et al.</i> [29] | Low | High |
| 4 | Proposed Model | High | High |

5.4. Text and image encryption/decryption

After make encryption and decryption in our proposed system we evaluate by using (PSNR, MSE, and BER) the result in this case shows the quality of image after decryption in proposed system is good. The make more than 5 experiments in image encryption and decryption, in our proposed system, we use RSA3k algorithm for text encryption and decryption. This algorithm requires 3 keys a public key and a private 2 key, a public key is used only for encryption, and the private key is used only for decryption. Will show the results of two experiments as show in Table 5.

Table 5. The experiments text and image encryption/decryption

| No | | Images and evaluation | | |
|----|----------------|---|--|---|
| 1 | Image 1 | Original | Encrypted | Decrypted |
| | PSNR | 58.9694 |  |  |
| | MSE | 0.0824 | | |
| | BER | 0 | | |
| | Time encrypt | 0.085478 | | |
| | Time decrypt | 0.039626 | | |
| | |  | | |
| 2 | Image 2 | Original | Encrypted | Decrypted |
| | PSNR | 65.5861 |  |  |
| | MSE | 0.0180 | | |
| | BER | 0 | | |
| | Time encrypt | 0.084077 | | |
| | Time decrypt | 0.021103 | | |
| | |  | | |
| 3 | Image 3 | Original | Encrypted | Decrypted |
| | PSNR | 67.0376 |  |  |
| | MSE | 0.0012 | | |
| | BER | 0 | | |
| | Time encrypt | 0.026895 | | |
| | Time decrypt | 0.089263 | | |
| | |  | | |
| 4 | Image 4 | Original | Encrypted | Decrypted |
| | PSNR | 68.4774 |  |  |
| | MSE | 0.0092 | | |
| | BER | 0 | | |
| | Time encrypt | 0.096635 | | |
| | Time decrypt | 0.028295 | | |
| | |  | | |
| 5 | Image 5 | Original | Encrypted | Decrypted |
| | PSNR | 75.2070 |  |  |
| | MSE | 0.0020 | | |
| | BER | 0 | | |
| | Time encrypt | 0.091629 | | |
| | Time decrypt | 0.024666 | | |
| | |  | | |

6. CONCLUSION AND FUTURE WORK

In this paper, a novel image security technique is intelligent system to encrypt and decrypt images as well as texts has been proposing; such system has combined two algorithms DCT and SR. In addition, using the RSA3k algorithm the proposed system has been compared with SR algorithm. Simulation results have proven that the proposed system performs better. The database loading has been and as a result the searching time has been reduced moreover, the recognition rate has been increased. In future work we will try to combine another algorithm with the presented system to improve the results providing higher security and quality as compared to existing techniques.




REFERENCES

- [1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. C. -Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.
- [2] S. Abt and H. Baier, "Are We Missing Labels? A Study of the Availability of Ground-Truth in Network Security Research," *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, 2014, pp. 40-55, doi: 10.1109/BADGERS.2014.11.
- [3] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378–403, 2013, doi: 10.1016/j.comnet.2012.07.021.
- [4] Ü. Çavuşoğlu, A. Akgül, S. Kaçar, İ. Pehlivan, and A. Zengin, "A novel chaos-based encryption algorithm over TCP data packet for secure communication," *Security and Communication Networks*, vol. 9, pp. 1285–1296, 2016, doi: 10.1002/sec.1414.
- [5] R. Sudhakar, R. Karthiga, and S. Jayaraman, "Image compression using coding of wavelet coefficients—a survey," *ICGST-GVIP Journal*, vol. 5, no. 6, pp. 25–38, 2005. [Online]. Available: https://static.aminer.org/pdf/PDF/000/320/249/adaptive_subband_image_coding_considering_spatial_relationship_on_hierarchical_pyramid.pdf
- [6] F. Li, L. Xin, Y. Liu, J. Fu, Y. Liu, and Y. Guo, "High efficient optical remote sensing images acquisition for nano-satellite framework," *Sensors, Systems, and Next-Generation Satellites XXI*, 2017, doi: 10.1117/12.2278171.
- [7] S. A. Shawkat, "Enhancing Steganography Techniques in Digital Images," Thesis, Faculty of Computers and Information, Mansoura University Egypt, 2016, doi: 10.13140/RG.2.2.16678.57925.
- [8] M. V. Rezende, "Evaluation of Face Recognition Technologies for Access Authentication in Automotive Passive Entry Systems with Near Infrared Camera," *Projetos e Dissertações em Sistemas de Informação e Gestão do Conhecimento*, vol. 4, 2015. [Online]. Available: <https://www.semanticscholar.org/paper/Evaluation-of-Face-Recognition-Technologies-for-in-Rezende/b051ffe615b55278eb9449cd6db543ce5fa3c288>.
- [9] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," *Future Generation Computer System*, vol. 72, pp. 273–287, 2017, doi: 10.1016/j.future.2016.08.018.
- [10] A. Nag *et al.*, "Image encryption using affine transform and XOR operation," *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*, 2011, pp. 309-312, doi: 10.1109/ICSCCN.2011.6024565.
- [11] F. Thabit, S. Alhomdy, A. H. A. Al-Ahdal, and S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Global Transitions Proceedings*, 2021, vol. 2, no. 1, pp. 91–99, doi: 10.1016/j.glt.2021.01.013.
- [12] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms," *3D Research*, vol. 8, no. 4, p. 37, 2017, doi: 10.1007/s13319-017-0148-5.
- [13] S. M. Seyedzade, S. Mirzakuchaki, and R. E. Atani, "A novel image encryption algorithm based on hash function," *2010 6th Iranian Conference on Machine Vision and Image Processing*, 2010, pp. 1–6, doi: 10.1109/IranianMVIP.2010.5941167.
- [14] M. Waschke, *Personal cybersecurity: how to avoid and recover from cybercrime*, Apress, 2017, doi: 10.1007/978-1-4842-2430-4.
- [15] N. A. Al-Otaibi and A. A. Gutub, "2-layer security system for hiding sensitive text data on personal computers," *Lecture Notes on Information Theory*, vol. 2, no. 2, pp. 151–157, 2014, doi: 10.12720/lnit.2.2.151-157.
- [16] I. Al Barazanhi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/telkomnika.v17i6.13201.
- [17] J. Shermina, "Illumination invariant face recognition using Discrete Cosine Transform and Principal Component Analysis," *2011 International Conference on Emerging Trends in Electrical and Computer Technology*, 2011, pp. 826-830, doi: 10.1109/ICETECT.2011.5760233.
- [18] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, 2017, doi: 10.1016/j.neucom.2016.12.038.
- [19] S. S. Hameed, H. R. Abdulshaheed, Z. L. Ali, and H. M. Gheni, "Implement DNN technology by using wireless sensor network system based on IOT applications," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 2, pp. 128-137, 2022, doi: 10.21533/pen.v10i2.2831.
- [20] D. Singh, I. Nath, and P. K. Singh, "Security and Privacy Challenges in Big Data," *Research Anthology on Privatizing and Securing Data. IGI Global*, 2021, doi: 10.4018/978-1-5225-9742-1.ch004.
- [21] Y. Yu *et al.*, "Cloud data integrity checking with an identity-based auditing mechanism from RSA," *Future Generation Computer System*, vol. 62, pp. 85–91, 2016, doi: 10.1016/j.future.2016.02.003.
- [22] S. A. Shawkat and R. N. Ismail, "Biometric Technologies in Recognition Systems: A Survey," *Tikrit Journal of Pure Science*, vol. 24, no. 6, 2019, doi: 10.25130/j.v24i6.899.
- [23] C. Thirumalai and H. Kar, "Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices," *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, 2017, pp. 1-6, doi: 10.1109/IPACT.2017.8244948.
- [24] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using AES," *International Journal for Innovative Research in Science and Technology*, vol. 2, no. 9, pp. 18–21, 2016. [Online]. Available: <https://www.semanticscholar.org/paper/Enhancement-of-Cloud-Computing-Security-with-Secure-Pancholi-Patel/71fad1cfde27b7df42e9b4579f9a623830893029>
- [25] M. Dalal and M. Juneja, "A secure and robust video steganography scheme for covert communication in H. 264/AVC," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 14383–14407, 2021, doi: 10.1007/s11042-020-10364-z.
- [26] S. A. Shawkat, K. S. L. Al-Badri, and A. I. Turki, "The new hand geometry system and automatic identification," *Periodicals of Engineering and National Science*, vol. 7, no. 3, pp. 996–1008, 2019, doi: 10.21533/pen.v7i3.632.




- [27] W. Wang and L. Xu, "A modified sparse representation method for facial expression recognition," *Computational Intelligence and Neuroscience*, vol. 2016, 2016, doi: 10.1155/2016/5687602.
- [28] S. Dabbaghchian, M. P. Ghaemmaghami, and A. Aghagolzadeh, "Feature extraction using discrete cosine transform and discrimination power analysis with a face recognition technology," *Pattern Recognition*, vol. 43, no. 4, pp. 1431–1440, 2010, doi: 10.1016/j.patcog.2009.11.001.
- [29] A. R. Chadha, P. P. Vaidya, and M. M. Roja, "Face recognition using discrete cosine transform for global and local features," in *2011 International Conference On Recent Advancements In Electrical, Electronics And Control Engineering*, 2011, pp. 502–505. doi: 10.1109/Iconraeece.2011.6129742.

BIOGRAPHIES OF AUTHORS



Shihab A. Shawkat    received the B.Sc. degree in Computer Science from University of Tikrit in 2007 and M.Sc. Degree in Computer Science from Mansoura University in 2017. Mr. Shihab A. Shawkat worked as a teacher during the period from 2008 to 2019 in Directorate of Education in Salah Al-Din, Ministry of Education, Iraq. He has recently started working at the University of Samarra at the end of 2019 till now. His research interest lies in Computer Science, Information Security, image processing and AI. He can be contacted at email: shahab84ahmed@gmail.com.



Israa Al-Barazanchi    received her Bachelor of Computer Science (BCS) from Department of Computer Science, Baghdad college of economic science university-Iraq-Baghdad in June 2002. In January 2010, she entered the master's program at the Faculty of Information and Communication Technology, Graduate School of Computer Science (Internetworking Technology), Universiti Teknikal Malaysia. She is Currently a student Doctor of Philosophy in Information and Communication Technology. She is a lecturer in Computer Engineering Techniques Department. Editor-in-chief for international union of universities journal. Member of Editor board in many Scopus journals for computer science field. Head of Researcher group. Member in many conferences panel and communications events. She is a Reviewer of various high impact factor journals. Her research activities are: WBAN, WSN, WiMAX, WiFi on Vehicular Ad-Hoc Networks (VANETs), Communications, Networking, Signal Processing, IOT, Smart Systems, Blockchain. She can be contacted at email: israa.albarazanchi@baghdadcollege.edu.iq and israa44444@gmail.com.