Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July, 2021:7376 – 7386

Research Article

Implementation of a Secured Student Record Management using Modified RC6 and OTP Algorithms

John Joseph G. Aguila[a], Ariel M.Sison[b], Ruji P.Medina[c], Catherine Bhel B. Aguila[d]

[a,d] Institute of Information Technology, Romblon State University, Romblon, Philippines
[b] School of Computer Studies, Emilio Aguinaldo College, Manila, Philippines
[c] Graduate Program, Technological Institute of the Philippines, Philippines
Email: [a]jaguila17@gmail.com, [b]ariel.sison@eac.edu.ph, [c]ruji.medina@tip.edu.ph, [d]cbaguila@rsu.edu.ph

Abstract

In today's generation, the utilization of multimedia for communication plays an important role in transmitting authentic messages over the network. However. its growth has also made easy distribution and duplication. Educational Institutions have salient academic documents which are official and highly confidential and institutions are intended to uphold their safety. This is achieved through FERPA or Family Educational Rights and Privacy Act which is one of the strongest privacy protection laws in the U.S while locally, the Philippines and its universities need to achieve their commitment to comply with the Data Privacy Act of 2012. The emerging increased use of applications such as Student Information System (SIS) and Learning Management Systems (LMS), consequently raised security concerns ensuring its confidentiality, integrity, and availability. It was based on the avalanche effect, correlation coefficient, mean squared error, and the speed measurement of encryption and decryption processes that the statistical and runtime execution analysis were conducted. The quality of encryption was improved as evidenced by the 54.69% avalanche effect, which surpasses the standard of 50%, a very low average correlation coefficient of 0.0022 for the horizontal, vertical and diagonal directions, and a high mean squared error (MSE) of 11,556. Minimal runtime was also achieved based on the encryption runtime average of 0.98 and decryption runtime average of 1.93. Based on the numerical and visual results of the actual runtime and automatic tests, the good qualities of encryption and authentication were achieved.

Keywords: *data security, modified RC6, one-time password, record management*

Introduction

Nowadays, the technology evolution drives the use of audiovisual aids over a computer network for communication and convey confidential information [1]. This growth has also made easy duplication and distribution of these multimedia data.

Educational Institutions have salient academic documents which are official and highly confidential and institutions are intended to uphold their safety. This is achieved through

FERPA or Family Educational Rights and Privacy Act which is one of the strongest privacy protection laws in the U.S while locally, the Philippines and its universities need to achieve its commitment to comply with the Data Privacy Act of 2012.

The traditional process of storing records often leads to unsecured paper or electronic records which is prone to some of the high dishonest practices such as falsification of results because of unauthorized disclosure.

For the past years, the growth in the education field in terms of student records is rapidly increasing. As a result, evolving application usage such as SIS and LMS in schools has recently increased especially the use of web and mobile applications to disseminate records of students among academic institutions. On the other hand, the usage of these technologies in disseminating student's records has elevated security issues on how to maintain confidentiality, integrity, and authenticity of data. [4], [5]

The protection of multimedia content sharing and transmission of student information via the internet has become an essential and difficult job [6]–[9]. Ensuring the data privacy of students and safeguarding their records must be one of the main roles that must be performed by every educational institution especially in this age of cyber-attacks where reports of breaches on data have become a common phenomenon [10].

Image data is one of the most confidential student records which has characteristics of large file size compared to text and strong correlations between adjacent pixels. The properties of image data include bulk capacity, high redundancy, and correlation between pixels. Thus, image encryption requires a higher requirement than text encryption [11]. Its efficiency and low computational complexity are essential in ensuring security in digital images [1]. Moreover, robust user authentication for remote users is needed for securing network access.

This study developed a secured student record management system (SSRMS) that integrates the modified RC6 encryption algorithm for online dissemination of student/alumni confidential records and applies a one-time password to achieve integrity for remote user's authentication.

Encryption And Authentication

In multimedia storage and transmission process over the network requires and enforces authentication, content access control, reliable and protection [1]. Image encryption is needed in transforming an image into unreadable information. This encryption technique offers a solution to security issues of multimedia like image processing [12]. There are two kinds of encryption such as asymmetric and symmetric encryptions. Asymmetric encryption performs much slower than symmetric encryption which requires higher computational complexity; thus, it is not suited for data management type of application [11]. While, symmetric encryption is proven acceptable when applied to still media information like images [1], [13] is to be secured.

A. RC6 Algorithm

It is an asymmetric encryption algorithm being one of the widely used today for protecting images [14], [15]. RC6 is known as a simple encryption algorithm when applied to text and image data. The RC6 algorithm is [PS3] considered as traditional encryption [16], [17] and is characterized as a simple encryption algorithm when applied to text and image data [18],

[19]. Several modifications have been developed by researchers to improve the quality and speed of the encryption and decryption processes [16], [20], [21].

B. One Time Password

OTP algorithm is one of the simplest and common forms of two-factor authentication utilized in network access security. Large enterprises often implement this technology in Virtual Private Network (VPN) access that often requires OTP access for user authentication on remote approach. OTP are often ideal to stronger forms of authentication such as PKI or biometrics because it does not require the installation of any client desktop software on the user machine. Thus, it allows to roam across multiple technologies including personal computers, personal digital assistants and kiosks [22].

Methodology

A. Design Specification

This study deals with the proposed design and development of SSRMS to implement the modified RC6 as a student record encryption scheme. A modified RC6 algorithm was produced with the use of cyclic shift as a new approach that improved the permutation-diffusion architecture of the standard RC6 in securing the image [21]. The system users were being verified and validated according to system restriction policies. On the system user side, the registrar's record officer is responsible for handling records according to who handles it and the cut-off policy. The filing system of student records was designed based on its categories whether it is permanent, temporary, or directory files.

A user account is verified and validated before the uploading of a student document as shown in Figure 1. Document management will be based on its categories and file naming convention to the student's name and identification number. Under system policy, the full access authority is assigned to the registrar's record officer. Records are encrypted once permitted by the system and being recorded in the system administrator's transaction history; this process is automatically done in system settings. The approval and storing process will follow.

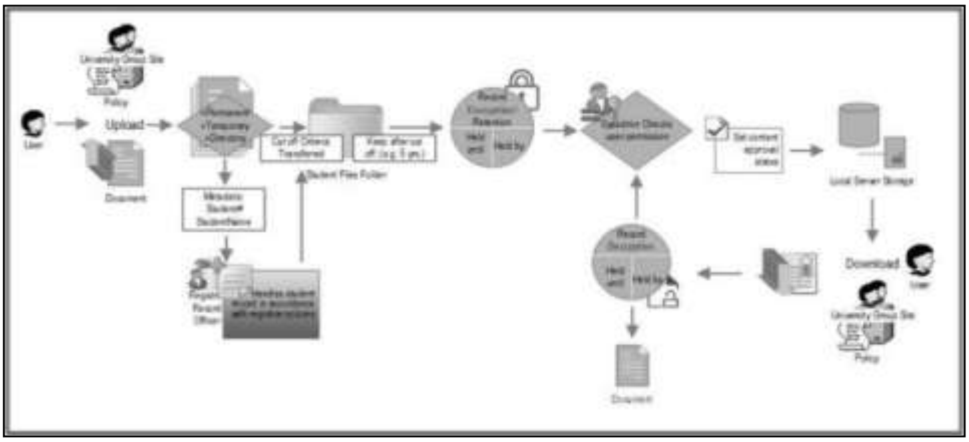


Figure 1. System Design Architecture

One of the core functions of the system is to process official document request online via system portal as presented in Figure 2.

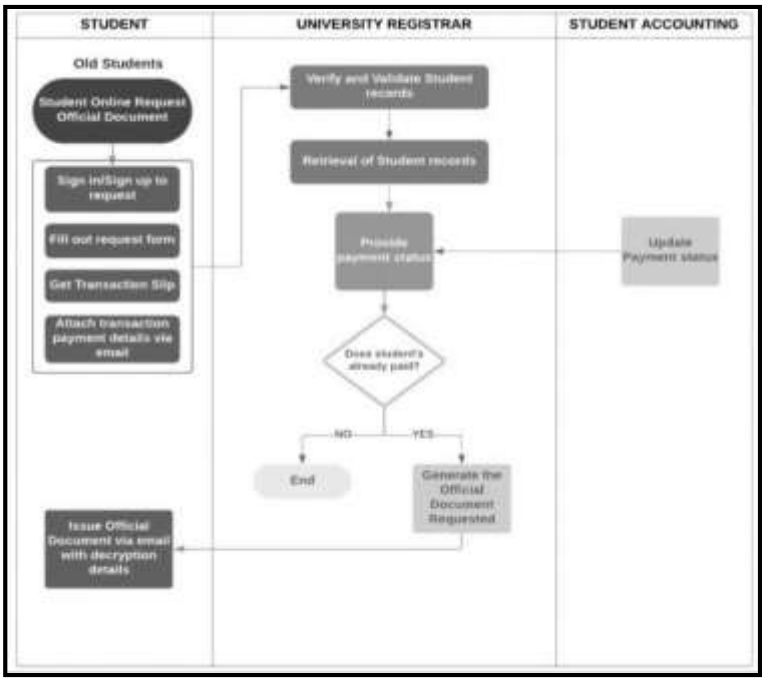

STUDENT
UNIVERSITY REGISTRAR
STUDENT ACCOUNTING
Old Students
Student Online Request Official Document
Sign in/Sign up to request
Fill out request form
Get Transaction Slip
Attach transaction payment details via email
Verify and Validate Student records
Retrieval of Student records
Provide payment status
Update Payment status
Does student's already paid?
NO
YES
End
Generate the Official Document Requested
Issue Official Document via email with decryption details

Figure 1. User Document Request Online

A student or an alumni can request an official document like transcript of record or diploma via portal by providing personal details that matches their student personal records. Valid identification must be attached for further validation. The pending request and payment details must be verified and validated by the university registrar before approval. Once approved, the system will send a secured download link to the verified email address of the student/alumni. The link is dedicated to one (1) email address and its validity once approved is 24 hours only.

A. Operational Design

The operational design stage includes user management, data preprocessing, key expansion, encryption, decryption and authentication.

User Management. Validation and verification of user accounts will be done to manage and access the student records as shown in Figure 1. Authorized users will be allowed to view and modify student records which are essential in validating, tracing, recording and monitoring its services. During installation of the system, it will automatically create essential user account which has different types such as system administrator, regular and guest user account.

Data Preprocessing. In Figure 1, each student has individual folders containing their records categorized as permanent, temporary and directory. Extraction of these records from the existing enrollment system database is applied. Preprocessing of text-based and image format has different approach wherein in text-based format, bit conversion is being executed first before encryption and vice versa for decryption. While, for image format data, conversion of plain image to grayscale is being executed first before encryption and vice versa for decryption.

Key Expansion. The defined keys of 16-byte characters will be used in the key expansion algorithm stage adopted from the original RC6 algorithm. In standard RC6 algorithm, to expand user key in order to fill an array S, the key expansion algorithm is used. The user must provide a key of b (bytes), and from which (2r+4) words are derived and stored in a round key array S. The key bytes are loaded into an array L[0,..,c-1] of c=ceil(b/u) where u=w/8 in little-endian order. Any vacant byte positions in L are zeroed [23]. The (2r+4) derived words are stored in array S[0,..,2r+3] for later encryption or decryption process. The magic constant Pw and Qw are defined for the arbitrary of (w) as shown in Table 1 [24].

TABLE 1. MAGIC CONSTANTS VALUES PW AND QW

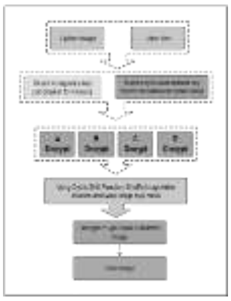
W	**Equation**	**16**	**32**	**64**
Pw	Pw=Odd((e-1) 2^w)	B7E1	B7E15163	B7E151628AED2A6B
Qw	Qw=Odd((v-1) 2^w)	9E37	9E3779B9	9E3779B97F4A7C15

Encryption. As shown in Figure 3(a), before encryption, image is converted to byte values and grayscale. A colored image conversion into grayscale is converting RGB values of 24 bits into grayscale value of 8 bit [25]. Image file size usually reduced almost more than 17% as shown in the sample result of converted image in Figure 3(c). User key is supplied to perform key expansion as adopted in standard RC6. Image is divided into blocks with 32-bit size assigned in four registers which are A, B, C, D registers. The six (6) encryption operations of the standard RC6 algorithm perform recommended 20 rounds of iterations. The transformed encrypted image is divided into four (4) blocks based on its image byte index value. The four (4) sets of 16- key sequence combination based on the image byte index value of each block is randomly generated. In each block, a separate key sequence combination is utilized as a pattern to shift the index location of the image cyclic shift permutation. Simultaneously, image byte value changes as diffusion mechanism. The corresponding output of image file encryption is shown in Figure 3(c).

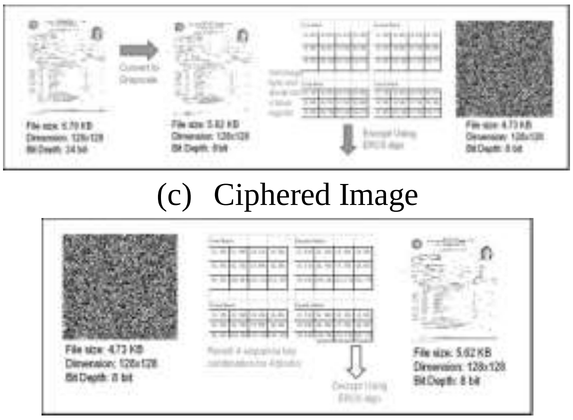
Decryption. As presented in Figure 3(b),the encrypted image is read and the secret key is entered to trigger the process of sequence key locator. The reverse operation of the cyclic shift permutation and diffusion-based is performed once located the sequence key that was mixed and hidden in cipher image attributes. Then, the adopted original decryption steps of the RC6 algorithm operations are performed to get the recovered image. The output of decrypted/deciphered image is shown in Figure 3(d).

Authentication. One-Time Password is a form of two-factor authentication that is used in this study for securing access to accounts. It is done by generation of synchronized One-Time Password (OTP) values based on SHA-1 based Hash Message Authentication Code (HMAC). One-Time Passwords are often referred to as a secure and stronger forms of authentication, and allowing them to installed across multiple machines including home computers, mobile phones, tablets and laptops. When the user attempts to login, an OTP is generated and sent to the user’s e-mail account. Then a user is directed to next page and is asked to enter the OTP from the e-mail account and enters it. Once OTP is verified, the user succeeds in logging in the system.

(a) RC6 Encryption Block Diagram



(b) RC6 Decryption Block Diagram



(c) Ciphered Image

(d) Deciphered Image

Figure 3. Encryption and Decryption Block Diagram and Generated Output

Results And Discussion

Correlation Coefficient. The result of the correlation coefficient of the four (4) test images and its corresponding encrypted image in three adjacent pixel directions of horizontal, vertical and diagonal are shown in Table 2.

TABLE 2. CORRELATION COEFFICIENT OF ADJACENT PIXELS OF PLAIN AND CIPHER IMAGE

Adjacent Pixel Direction	Lena.jpg		Monkey.jpg		Pepper.jpg		Plane.jpg	
	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image
Horizontal	0.9277	0.0050	0.9106	0.0006	0.9635	0.0042	0.8605	-0.0068
Vertical	0.9656	-0.0140	0.9084	0.0340	0.9458	-0.0049	0.8698	0.0135
Diagonal	0.9097	0.0133	0.9117	-0.0203	0.9688	0.0188	0.8747	-0.0168
Average	**0.9343**	**0.00143**	**0.9102**	**0.00477**	**0.9594**	**0.0060**	**0.8683**	**-0.0034**

The zero value or negative correlation result values of the cipher image indicates that color attributes have less or no correlation at all meaning the image is hidden or unrecognized, while plain image correlation value is close to

1. There are negative result values of adjacent pixel value distribution in three different directions of four cipher images. In the horizontal direction, the lowest value was achieved by Plane image while in diagonal direction Monkey and Plane images achieved the lowest adjacent values. The vertical direction for both Lena and Pepper images achieved the lowest values.

The correlation result values of the plain image were close to 1 while the cipher images have less correlation which is very close to 0 or even negative result which all indicate very good performance in hiding the image attributes [26]

Avalanche Effect. The significant change in two cipher texts in this study presented the avalanche effect and occurred even a 1-bit change in the next plaintext input. The result presented the number of flipped bits between two plaintexts. The summary of results is shown in Table 3. The calculated average number of flipped bits per byte (8 bits) as shown in Table 3 have result value of 4.48 bits (out of 8 bits) based on the two cipher texts with single bit difference, which surpasses the standard minimum threshold of 50% [27].

Mean Squared Error. The MSE parameter presented results that calculated the squared error or difference achieved by the two encrypted output with single bit difference in the defined key is shown in Table 4.

TABLE 3. AVALANCHE RESULT OF TWO CIPHER TEXT (128-BIT)

Ciphertext 1 (Byte)	Ciphertext 2 (Byte)	Number of Flipped Bits per Byte
1100101	1010010	5
1000010	1100101	4
10010000	11000001	3
111011	11000111	6
1010000	11010	3
110110	11010	3
11001100	11011000	2
1110010	11010000	3
10100100	11100101	2
1000111	11111101	5
11110101	10110010	4
00011010	11101110	6
00101000	11010001	6
10110111	1001101	6
10100011	1100000	4
11010011		8
Average Number of Flipped bits per byte	**4.48**	

TABLE 4. MEAN SQUARE ERROR RESULT

Image Data	MSE	PSNR
Lena.jpg	11417.08	7.59 dB
Monkey.jpg	11720.44	7.48 dB
Pepper.jpg	11592.97	7.52 dB
Plane.jpg	11493.9	7.56 dB
Average	**11556.1**	**7.54 dB**

The results presented in Table 4 showed higher MSE values which indicate higher difference even with 1-bit difference used in the defined key [28], [29]. PSNR or Peak Signal to Noise Ratio values were included which also showed that its low result value yields better encryption [30] which truly hides the plain image.

Runtime Execution. The encryption and decryption run-times are presented in Table 5 when using the enhanced RC6 prototype with K1=12345678ABCDEFGH as the secret key, 128x128 image dimension, parameter value of 20 rounds, and 128-bit encryption per block.

TABLE 5. EXECUTION TIME RESULTS OF MODIFIED RC6 (IN SECONDS)

.jpg test images	**Encryption Time**	**Decryption Time**
Lena	0.99	1.90
Monkey	0.98	1.90
Pepper	0.98	1.95

Plane	0.98	1.97
Average	**0.98**	**1.93**

Conclusion And Recommendation

The modified RC6 algorithm is an efficient encryption algorithm when applied to student records which are converted to image files without sacrificing the processing time. The statistical analysis of the modified RC6 algorithm exhibits good encryption quality achieving an avalanche effect of 54.69%. There is a very low correlation coefficients of 0.00075 for the horizontal direction, -0.00125 for the diagonal direction, and 0.00715 for the vertical direction which all indicate very good performance in hiding the image attributes; and a very high mean squared error of 11,557 which indicates higher intensity of change even for a single bit difference between two encrypted images. Integrating OTP algorithm also achieved the security over network access. Future work of this study is to further test the functionality and efficiency of the system based on user needs.

References

[1] A. Rasmi, B. Arunkumar, and V. M. Anees, “A Comprehensive Review of Digital Data Hiding Techniques,” Pattern Recognit. Image Anal., vol. 29, no. 4, pp. 639–646, 2019.

[2] W. Garner and W. Garner, “FERPA, HIPAA, and Other Privacy Concerns in Online Education,” EdMedia + Innov. Learn., vol. 2018, no. 1, pp. 519–523, 2018.

[3] B. Akiwate, A. Patel, T. Nabiwale, N. Naik, and S. Patil, “Web Based Student Information Management System using MEAN Stack,” 2016.

[4] K. M. L. Jones et al., “‘We’re being tracked at all times’: Student perspectives of their privacy in relation to learning analytics in higher education,” J. Assoc. Inf. Sci. Technol., 2020.

[5] M. Brown and C. Klein, “Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents,” J. Higher Educ., 2020.

[6] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.

[7] Y. Liu, J. Wang, J. Fan, and L. Gong, “ Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences,” Multimed. Tools Appl., 2016.

[8] J. Y. Effa, J. De, D. Nkapkop, M. Cislariu, and M. Borda, “Comparative Analysis of Different Structures of Chaos- Based Cryptosystems: A Survey,” vol. 57, no. 2, 2016.

[9] I. Lin and T. Liao, “A Survey of Blockchain Security Issues and Challenges,” vol. 19, no. 5, pp. 653–659, 2017.

[10] K. Burden, M. Kearney, S. Schuck, and T. Hall, “Investigating the use of innovative mobile pedagogies for school-aged students: A systematic literature review,” Comput. Educ., vol. 138, no. April, pp. 83–100, 2019.

[11] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, “Comprehensive study of symmetric key and asymmetric key encryption algorithms,” in Proceedings of2017 International Conference on Engineering and Technology, ICET 2017, 2018.

[12] H. V. Gamido, A. M. Sison, and R. P. Medina, “Implementation of modified aes as image encryption scheme,” Indones. J. Electr. Eng. Informatics, 2018.

[13] M. Khan and T. Shah, “ A Literature Review on Image Encryption Techniques ,” 2014.

[14] A. B. Mohamed, G. Zaibi, and A. Kachouri, “An Efficient RC6 based Image Cryptography to Enhance Correlation and Entropy,” Int. Multi-Conference Syst. Signals Devices, SSD’11 - Summ. Proc., 2011.

[15] A. Shrivastava, “An Efficient RC6 based Image Cryptography to Enhance Correlation and Entropy,” vol. 139, no. 1, pp. 42–49, 2016.

[16] P. Chaturved, “An Enhanced Secure Image Cryptography based on RC6 and RSA to Minimize Entropy and Improve Correlation,” Int. J. Eng. Comput. Sci., vol. 5, no. 10, pp. 18293–18301, 2016.

[17] S. Contini, R. L. Rivest, and M. J. B. Robshaw, “Some Comments on the First Round AES Evaluation of RC6,” 1998.

[18] A. H. M. Ragab, O. S. F. Alla, and A. Y. Noaman, “Encryption Quality Analysis of the RCBC Block Cipher Compared with RC6 and RC5 Algorithms.,” IACR Cryptol. ePrint Arch., vol. 2014, p. 169, 2014.

[19] H. K. Verma, “Enhancement of RC6 Block Cipher Algorithm and Comparison with RC5 & RC6,” pp. 556–561, 2012.

[20] K. Aggarwal and A. K. Expansion, “Comparison of RC6, Modified RC6 {&} Enhancement of RC6,” pp. 444–449, 2015.

[21] C. B. B. Aguila, A. M. Sison, and R. P. Medina, “Enhanced RC6 Permutation-Diffusion Operation for Image Encryption,” inIn Proceedings of the 2018 International Conference on Data Science and Information Technology (DSIT ’18).ACM, New York, NY, USA, 2018, pp. 64–68.

[22] K. N. Sivabalan and S. Balakrishnan, “Securing Sensitive Web Based Student Academic Performance System with Base64 Encoding and Systematic Mirroring,” vol. 119, no. 12, pp. 1117–1126, 2018.

[23] H. K. Verma and R. K. Singh, “Enhancement of RC6 block cipher algorithm and comparison with RC5 &amp;amp; RC6,” in2013 3rd IEEE International Advance Computing Conference (IACC), 2013, pp. 556–561.

[24] H. K. Verma and R. K. Singh, “Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6,” Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. IACC 2013, pp. 556–561, 2013.

[25] C. Saravanan, “Color Image to Grayscale Image Conversion,” in 2010 Second International Conference on Computer Engineering and Applications, 2010, pp. 196–199.

[26] N. Ahmed, H. M. Shahzad Asif, and G . Saleem, “ A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes ,” Int. J. Comput. Netw. Inf. Secur., vol. 8, no. 12, pp. 28–29, 2016.

[27] A. K. Mandal, C. Parakash, and A. Tiwari, “Performance evaluation of cryptographic algorithms: Des and AES,” in 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science: Innovation for Humanity, SCEECS 2012, 2012.

[28] J. Ahmad and F. Ahmed, “ Efficiency analysis and security evaluation of image encryption schemes ,” Computing, vol. 23, no. 04, p. 25, 2010.

[29] Y. Wang, K. Wong, X. Liao, and G. Chen, “A new chaos-based fast image encryption algorithm,” vol. 11, pp. 514–522, 2011.

[30] Shankar K. and Eswaran P., “Sharing a Secret Image with Encapsulated Shares in Visual Cryptography,” Procedia Comput. Sci., vol. 70, pp. 462–468, Jan. 2015.