

A novel cryptographic scheme based on the ES transform

Rusul Ahmed Flayyih *

Suha Raisan Harbi [†]

General Directorate of Education Thi-Qar

Ministry of Education

Thi-Qar

Iraq

Ahlam Abdulkareem Mahdi [§]

Huda Ali Falih [‡]

General Directorate of Education Najaf

Ministry of Education

Najaf

Iraq

Emad Abbas Kuffi [@]

Department of Mathematics

College of Basic Education

Mustansiriyah University

Baghdad

Iraq

Abstract

In this paper, a novel cryptographic approach based on the ES transform is proposed for secure text encryption and decryption. The method employs the Emad–Sara transforms to convert plaintext into an encrypted representation, thereby enhancing data confidentiality through mathematical transformation. Decryption is achieved by applying the corresponding inverse ES integral transform, which enables accurate recovery of the original plaintext without information loss. The proposed scheme is illustrated with a detailed numerical example that demonstrates both the encryption and decryption processes. The results confirm the correctness, reversibility, and computational feasibility of the method. Owing

* E-mail: mskmrtdy588@gmail.com (Corresponding Author)

[†] E-mail: suhamaster7@gmail.com

[§] E-mail: ahlamalfaisaly@gmail.com

[‡] E-mail: hudaali2020aledani@gmail.com

[@] E-mail: emad.Kuffi@uomustansisiyah.edu.iq

to its transform-based structure, the approach provides an additional layer of security and shows potential for integration into modern cryptographic systems. This study highlights the applicability of the Emad–Sara transforms as a practical mathematical tool for information security and opens avenues for further research into their robustness and performance in advanced encryption frameworks.

Subject Classification: 94A60, 11T71.

Keywords: ES-integral transform, Inverse ES-transform, Cryptography, Cryptosystem, Encryption, Decryption.

1. Introduction

Encryption is a cybersecurity measure that keeps sensitive information secure by using unique codes that scramble data, making it unreadable to hackers [1]. Private data is protected within an organization through encryption; even if attackers bypass the firewall, the encrypted data remains protected. A large amount of private user data is increasingly collected by companies, and data encryption is used to protect it [2]. To protect this data from unauthorized access, companies must ensure that they encrypt all information in their possession. Information is encrypted straightforwardly using encryption keys and a secret encryption algorithm to convert unencrypted text into encrypted text [3-6].

The most effective method to secure the data is to transform the message from a form understandable to all parties into one that can be read only by the intended parties. This method is said to be cryptography [7-10].

In the cryptographic system, the side that would send the data (the source) should encrypt the data using encryption and decryption keys, and the resulting ciphertext would be sent over an insecure channel. The receiving side of the decryption key [11-14]. ES-Integral transform has been used in many scientific fields. The ES integral transform is an effective tool for cryptography. In this work, a new cryptographic system based on the ES-transform is discussed and illustrated with an example.

2. ES-Integral Transform

If $f(t)$, $t \geq 0$ is a function having an exponential order that be a continuous function on interval, so ES-Integral transforms for the $f(t)$ is:

$$E\{f(t)\} = T(\psi) = \frac{1}{\psi^2} \int_{t=0}^{\infty} e^{-\psi t} f(t) dt.$$

2.1 Applying ES-Integral Transform in Some Basic Functions

$$E\{t^n\} = \frac{n!}{\psi^{n+3}}, \text{ where } n = 0, 1, 2, 3, \dots$$

$$E\{e^{bt}\} = \frac{1}{\psi^2(\psi-b)}, \text{ for constant } b.$$

$$\begin{aligned}
E\{\sin(bt)\} &= \frac{b}{\psi^2(\psi^2+b^2)} \cdot \\
E\{\cos(bt)\} &= \frac{b}{\psi(\psi^2+b^2)} \cdot \\
E\{\sinh(bt)\} &= \frac{b}{\psi^2(\psi^2-b^2)} \cdot \\
E\{\cosh(bt)\} &= \frac{1}{\psi(\psi^2-b^2)} \cdot \\
E\{\delta(t)\} &= \frac{1}{\psi^2} \cdot \\
E\{f'(t)\} &= \frac{-f(0)}{\psi^2} + \psi T(\psi) \cdot \\
E\{f''(t)\} &= \frac{-f'(0)}{\psi^2} + \psi E\{f'(t)\} \cdot \\
E\{f^n(t)\} &= \frac{-f^{n+1}(0)}{\psi^2} + \psi E\{f^{n-1}(t)\} \cdot
\end{aligned}$$

2.2 Inverse ES-Integral Transform

The inverse ES-Integral transform of some main functions are:

$$\begin{aligned}
E^{-1}\{\psi^{n+3}\} &= \frac{t^n}{n!}, n = 0,1,2,3, \dots \\
E^{-1}\left\{\frac{1}{\psi^2(\psi-b)}\right\} &= e^{bt}, b \text{ is a constant} \cdot \\
E^{-1}\left\{\frac{1}{\psi^2(\psi^2+b^2)}\right\} &= \frac{1}{b} \sin(bt) \cdot \\
E^{-1}\left\{\frac{1}{\psi(\psi^2+b^2)}\right\} &= \cos(bt) \cdot \\
E^{-1}\left\{\frac{1}{\psi^2(\psi^2-b^2)}\right\} &= \frac{1}{b} \sinh(bt) \cdot \\
E^{-1}\left\{\frac{1}{\psi(\psi^2-b^2)}\right\} &= \cosh(bt) \cdot
\end{aligned}$$

3. Proposed Methodology

The cryptographic method contains the following:

1. In this way, we are going to use a key system that includes encryptions and decryptions key, which identified only to a transmitter part and receivers part.
2. A data be process in cryptographic methods be encode in MURUSL codes.
3. ES-transform has been applied at the sender party of encryption, and inverse ES-transforms be applied at receive party as parts for the decryptions.

4. Encryption Algorithm

We should be performed the following steps at the transmitter part to transforms message from it is understand into not understand form (illegible) message.

Step 1: Take each letters in plain text as the numbers, s.t A=1, B=2, C=3, Z=26.

Step 2: messages be very organize finite sequences for the previous conversion.

For Example, the encoding MURUSL codes. Take M=10, U=5, R=2, S=6, L=5 hence our plain text sequence is 10, 5, 2, 6, 5.

Step 3: If the sum of term in the sequence is $n+1$ assume a polynomials for the degree n with coefficients as terms for the finite sequences.

A previous finite sequences includes 5+1 of term then regard a polynomial $f(t)$ of degree 5,

$$f(t) = 10 + 5t + 2t^2 + 6t^3 + 5t^4.$$

Step 4: Take ES-transform of polynomial $f(t)$;

$$\begin{aligned} E[f(t)] &= E[10 + 5t + 2t^2 + 6t^3 + 5t^4] \\ &= \frac{10}{\beta^3} + 5 \left(\frac{t}{\beta^4} \right) + 2 \left(\frac{2!t^2}{\beta^5} \right) + 6 \left(\frac{3!t^3}{\beta^6} \right) + 5 \left(\frac{4!t^4}{\beta^7} \right). \\ &= \frac{10}{\beta^3} + \frac{5t}{\beta^4} + \frac{4t^2}{\beta^5} + \frac{36t^3}{\beta^6} + \frac{120t^4}{\beta^7} = \sum_{i=1}^{5+1} \frac{\mu_i}{\beta^{i+1}}. \end{aligned}$$

Step 5: Now find τ such that $\mu_i = \tau i \bmod 26$. for each $i = 1, 2, 3, \dots$ therefore $\mu_1 = 10 \equiv 10 \bmod 26$, $\mu_2 = 5 \equiv 5 \bmod 26$, $\mu_3 = 4 \equiv 4 \bmod 26$, $\mu_4 = 36 \equiv 10 \bmod 26$, $\mu_5 = 120 \equiv 16 \bmod 26$.

Step 6: Take $i = 26ki + \tau i$, so fore key ki where $i = 1, \dots, n+1$.

Then $k_1 = 0, k_2 = 0, k_3 = 0, k_4 = 10, k_5 = 16$.

Step 7: we consider a finite sequence a new $\tau_1, \tau_2, \dots, \tau_{n+1}$. i.e 10, 5, 4, 10, 16.

5. Decryption Algorithm

The cryptosystem's mathematical method is explained by the decryption algorithm. The next Example will explain it.

Step 1: Consider the secret text receive from the sender in previous Examples secret text be the MURUSL codes, the key be 0, 0, 0, 10, 16.

Step 2: Consider the given secret text as an equivalent finite sequence $\tau_1, \tau_2, \tau_3, \dots, \tau_{n+1}, 10, 5, 4, 10, 16$.

Step (3): Let $\mu_i = 26ki + \tau_i, \forall i = 1, 2, 3, \dots, n+1$, $\mu_1 = 26(0) + 10 = 10$, $\mu_2 = 26(0) + 5 = 5$, $\mu_3 = 26(0) + 4 = 4$, $\mu_4 = 26(10) + 10 = 270$, $\mu_5 = 26(16) + 16 = 432$.

Step 4: Let

$$\mu(\beta) = \sum_{i=1}^{n+1} \frac{\mu i}{\beta^{n+1}} = \frac{10}{\beta^3} + \frac{5}{\beta^4} + \frac{4}{\beta^5} + \frac{10}{\beta^6} + \frac{16}{\beta^7}.$$

$$10\left(\frac{0!}{\beta^3}\right) + 5\left(\frac{1!}{\beta^4}\right) + 2\left(\frac{2!}{\beta^5}\right) + 6\left(\frac{3!}{\beta^6}\right) + 5\left(\frac{4!}{\beta^7}\right).$$

Step 5 : Take the inverse ES-transform of $f(\beta)$ then

$$E^{-1}[f(t), t] = E^{-1}\left[10\left(\frac{0!}{\beta^3}\right) + 5\left(\frac{1!}{\beta^4}\right) + 2\left(\frac{2!}{\beta^5}\right) + 6\left(\frac{3!}{\beta^6}\right) + 5\left(\frac{4!}{\beta^7}\right)\right].$$

$$f(t) = 10 + 5t + 2t^2 + 6t^3 + 5t^4$$

Step 6: Suppose coefficient for polynomials $f(t)$ are finite sequences 10, 5, 2, 6, 5.

6. Conclusions

A cryptographic methodology using the ES-Integral transform has been recommended; it is generic in nature. To recognize this recommended methodology, a useful example is encrypting a message using encryption algorithms, then decrypting; the result shows the capability of applying the ES-transform in the encryption field to obtain information.

A video encoding and encoding expert does not consider the viewer to be of the experts knowledge of the algorithm or method relied upon to encode between message data, where an infinite number of algorithms have been found to search for their statistics and not monitor others by hacking them, which is a simple process by trying to understand the rose that could be used by ancient civilizations to document their cultures and they; It is necessary to analyze these symbols and put hypotheses around them Nicole computer tools symbols to try to determine which ones are what unless the key is obtained.

References

- [1] S. F. Maktoof, E. Kuffi, and E. S. Abbas, "Emad-Sara Transform" a new integral transform," *Journal of Interdisciplinary Mathematics*, vol. 24, no. 7, pp. 1985–1994 (2021).
- [2] E. A. Mansour, S. Mehdi, and E. A. Kuffi, "The new integral transform and its applications," *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. 2, pp. 849–856 (2021).
- [3] M. T. Gençoğlu, "Use of integral transform in cryptology," *Science and Eng. J of Firat Univ*, vol. 28, no. 2, pp. 217–220 (2016).
- [4] M. T. Gençoğlu, "Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions," *Communications in Mathematics and applications*, vol. 8, no. 2, p. 183 (2017).

- [5] G. N. Lakshmi, B. R. Kumar, and A. C. Sekhar, "A cryptographic scheme of Laplace transforms," *International Journal of Mathematical Archive*, vol. 2, no. 12, pp. 2515–2519 (2011).
- [6] M. Mohand and A. Mahgoub, "The new integral transform 'Mohand Transform,'" *Advances in Theoretical and Applied Mathematics*, vol. 12, no. 2, pp. 113–120 (2017).
- [7] C. H. Jayanthi and V. Srinivas, "Mathematical Modelling for Cryptography using Laplace Transform," *International Journal of Mathematics Trends and Technology (IJMTT)*, vol. 65, no. 2, pp. 10-15 (2019).
- [8] C. Paar and J. Pelzl, *Understanding cryptography: A textbook for students and practitioners*. Berlin, Germany: Springer, (2009), doi: 10.1007/978-3-642-04101-3.
- [9] A. Kahate, *Cryptography and network security*. New York, USA: Tata McGraw-Hill Education, (2013).
- [10] A. Kamal and H. Sedeeg, "The new integral transform Kamal transform," *Advances in Theoretical and Applied Mathematics*, vol. 11, no. 4, pp. 451–458 (2016).
- [11] A. K. H. Sedeeg, M. M. Abdelrahim Mahgoub, and M. A. SaifSaeed, "An application of the new integral 'aboodh transform' in cryptography," *Pure and Applied Mathematics Journal*, vol. 5, no. 5, pp. 151–154 (2016).
- [12] A. Stanoyevitch, *Introduction to cryptography with mathematical foundations and computer implementations*. Boca Raton, FL, USA: CRC Press (2010).
- [13] P. S. Kumar and S. Vasuki, "An Application of MAHGOUB Transform in Cryptography," *Adv. Theor. Appl. Math*, vol. 13, no. 2, pp. 91-99 (2018).
- [14] W. Zhang, Y. Zhao, and S. Fan, "Cryptosystem identification scheme based on ASCII code statistics," *Security and Communication Networks*, vol. 2020, no. 1, Art. no. 8875864 (2020).

Received November, 2025