Applying Complex SEE Transformation in Cryptography

Eman A. Mansour[1*], Emad A. Kuffi[2], Sadiq A. Mehdi[3]

[1,3] *College of Education, Department of Mathematics, Mustansiriyah University, Baghdad Iraq.*

[2] *College of Engineering, Department of Material Engineering, Al-Qadisiyah University, Iraq.*

**Corresponding author: iman.am_73@uomustansiriyah.edu.iq*

Received 20-8-2021, Accepted 7-10-2021, published 31-12-2021.
DOI: 10.52113/2/08.02.2021/99-104

Abstract: In this paper, the capability of complex SEE (Sadiq-Emad-Emad) integral transform to be used in cryptography has been demonstrated, discussed and proven by practical example, in which the complex SEE transform had been used to encrypt a message and then decrypt the resulted ciphertext back into the original text.

Keywords: complex SEE integral transform, inverse complex SEE integral transform, cryptography, decryption, encryption.

1. Introduction

Data security represents an essential industrial pillar in the modern era, enterprise companies perform a great amount of researches to find the most suitable methods to protect data and reduce the threats directed form different types of adversaries to accommodates different agendas. Cryptography represents an important part of data security and it take place in most applications that involve data transition, however, cryptography had early start with the beginning of the persistent desire of humankind to keep some information private, even if it had been compromised by outsiders, there are many forms of cryptography, started from the classical methods to the modern more advanced methods.[1]

In applied mathematics, an integral transformation is a useful device in converting one function $g(t)$ into another of new variables $g(v)$, $g(s)$, etc. integral transformation had been used for a long time in many fields, such as, applied mathematics, natural sciences and engineering fields [2-7]. Integral transform had been also

used in the cryptography field, where they had been applied into exponential functions for the preposes of encryption and decryption [8-10].

In this work, complex SEE transformation, as a promising new integral transform has been used in the cryptography field, to encrypt a plaintext and then decrypt the resulted ciphertext.

2. Complex SEE Transformation [2-5]

Consider a function $g(t)$ of exponential order in the set B defined by: $B = \{g(t): \exists M, l_1, l_2 > 0 \,.\, |g(t)| < M^{-iL_j|t|}\,, if\ t \in (-1)x[0,\infty)\}$. Where i is a complex number, $i^2 = -1$.

For the given function in the set B, the constant M must be finite number, $l_1\ and\ l_2$ may be finite or infinite.

Complex SEE integral transform denoted by the operator S^cformula is defined by: $S^c\{g(t)\} = \frac{1}{v^n}\int_{t=0}^{\infty} g(t)e^{-ivt}\,dt = T(iv)\ ,\ t \geq 0\ ,\ l_1 \leq v \leq l_2\ ,\ n \in \mathbb{Z}$

The variable (iv) in the complex SEE transform is used to factor the variable t in the argument of the function $g(t)$.

2.1. Linearity Property of Complex SEE Transform, [2-5]

Complex SEE integral transform is a linear integral transform: $S^c\{\alpha g_1(t) + \beta g_2(t)\} = \alpha S^c\{g_1(t)\} + \beta S^c\{g_2(t)\}$. Where α, β are constants. The equation can be generalized to more than two functions.

2.2. Complex SEE Transformation and Inverse Complex SEE Transformation for Some functions, [2-5]

(1) $S^c\{C\} = -\frac{iC}{v^{n+1}}$,

$where\ C\ is\ a\ constant$

(2) $S^c\{t\} = -\frac{1}{v^{n+2}}$.

(3) $S^c\{t^2\} = \frac{(2!)i}{v^{n+3}}$.

(4) $S^c\{t^3\} = \frac{(3!)}{v^{n+4}}$. In general:

$S^c\{t^m\} = \frac{(-1)^m(i)^{m-1}(m!)}{v^{n+m+1}}$. Where $m \in \mathbb{N}$.

(5) $S^{c^{-1}}\left\{\frac{-i}{v^{n+1}}\right\} = 1$,

(6) $S^{c^{-1}}\left\{\frac{(-1)^m(i)^{m-1}(m!)}{v^{n+m+1}}\right\} = t^m$.

3. The Methodology of using complex SEE Transform in Cryptography

This section provides an insight to the procedure of using complex SEE transform in cryptographic scheme, including encryption and decryption.

3.1. Encryption Procedure

This procedure is performed by the sender, in which the encryption is performed on the data to transform it from coherent into incoherent data.

(1) Converting each letter in the plaintext into its equivalent sequential number in the alphabet, so that: A=0, B=1, C=2, D=3, …, Z=25.

(2) Organizing the plaintext as finite sequence of numbers based on the above conversion, for example the letters of text "TEASHERS" is converted into their equivalent numbers in the alphabet to become: T=20, E=5, A=1, H=8, R=18, S=19. Therefore, the plain text finite sequence is: (20,5,1,3,8,5,18,19).

(3) If $(s+1)$ is the number of terms in the plaintext sequence, then it is possible to generate a polynomial $p(x)$ of degree (s) with coefficient as the term of given finite sequence. For the taken example the finite sequence has $(7+1)$ terms, so that the polynomial $p(x)$ is of degree (7).

$p(x) = 20 + 5x + x^2 + 3x^3 + 8x^4 + 5x^5 + 18x^6 + 19x^7$.

(4) Taking complex SEE integral transformation for the polynomial $p(x)$: $S^c\{p(x)\} = S^c\{20\} + 5S^c\{x\} + S^c\{x^2\} + 3S^c\{x^3\} + 8S^c\{x^4\} + 5S^c\{x^5\} + 18S^c\{x^6\} + 19S^c\{x^7\}$,

$S^c\{p(x)\} = \frac{-20i}{v^{n+1}} - \frac{5}{v^{n+2}} + \frac{(2!)\,i}{v^{n+3}} + (3)\frac{(3!)}{v^{n+4}} - (8)\frac{(4!)\,i}{v^{n+5}} - (5)\frac{(5!)}{v^{n+6}} + (18)\frac{(6!)\,i}{v^{n+7}} + (19)\frac{7!}{v^{n+8}}$,

$S^c\{p(x)\} = \frac{(-20)i}{v^{n+1}} - \frac{5}{v^{n+2}} + \frac{(2)i}{v^{n+3}} + \frac{18}{v^{n+4}} - \frac{(192)i}{v^{n+5}} - \frac{600}{v^{n+6}} + \frac{(12960)i}{v^{n+7}} + \frac{95760}{v^{n+8}} = \sum_{k=1}^{8}\frac{(-1)^k(i)^k q_k}{v^{n+k}}$.

(5) finding r_k so that: $(q_k \equiv r_k mod\ 26)\ \ \forall k\,, (k = 1,2,\dots,s+1)$. Therefore:

$q_1 \equiv 20\ mod\ 26$, $q_2 \equiv 5\ mod\ 26$, $q_3 \equiv 2\ mod\ 26$, $q_4 \equiv 18\ mod\ 26$, $q_5 \equiv 192\ mod\ 26$, $q_6 \equiv 600\ mod\ 26$, $q_7 \equiv$

$12960\ mod\ 26$, $q_8 \equiv 95760\ mod\ 26$.

(6) Hence $(q_k = 26\delta_k + r_k)$. Thus, the key δ_k for $(k = 1,2,3, \dots, s+1)$ is: $\delta_1 = \delta_2 = \delta_3 = \delta_4 = 0\ and\ \delta_5 = 7$, $\delta_6 = 23$, $\delta_7 = 498\ and\ \delta_8 = 3683$.

(7) The encryption process produced a new finite sequence: $(r_1, r_2, \dots, r_{s+1}) = (20,5,2,18,10,2,12,2)$.

3.2. Decryption Technique

This procedure is performed by the receiver, in which the decryption is performed on the ciphertext to transform it back into coherent data.

(1) The ciphertext is received from the sender, that has prior knowledge of the encryption key, that has been received through a secure channel. In the above example ciphertext is "TEBRJBLB" and the key is $(0,0,0,0,7,23,498,3683)$.

(2) Converting the received ciphertext to the corresponding finite sequence of numbers: $(r_1, r_2, r_3 \dots, r_{s+1}) = (20, 5, 2, 18, 10, 2, 12, 2)$.

(3) Hence $(q_k = 26\delta_k + r_k\ \forall\ (i = 1,2,3, \dots, s+1)$. Then: $q_1 = 20$, $q_2 = 5$, $q_3 = 2$, $q_4 = 18$, $q_5 = 192$, $q_6 = 600$, $q_7 = 12960$, $q_8 = 95760$.

(4) Applying inverse complex SEE integral transformation of $P(v)$:

$$S^{c-1}\{P(v), x\} = S^{c-1}\left\{\frac{-20(0!)\ i}{v^{n+1}}\right\} + S^{c-1}\left\{\frac{-5(1!)}{v^{n+2}}\right\} + S^{c-1}\left\{\frac{(2!)\ i}{v^{n+3}}\right\} + S^{c-1}\left\{\frac{3(3!)}{v^{n+4}}\right\} + S^{c-1}\left\{\frac{-8(4!)\ i}{v^{n+5}}\right\} + S^{c-1}\left\{\frac{-5(5!)}{v^{n+6}}\right\} + S^{c-1}\left\{\frac{(18)(6!)\ i}{v^{n+7}}\right\} + S^{c-1}\left\{\frac{19(7!)}{v^{n+8}}\right\}$$

Then: $p(x) = 20 + 5x + x^2 + 3x^3 + 8x^4 + 5x^5 + 18x^6 + 19x^7$.

(5) Considering the coefficient of polynomial p(x) as finite sequence, translating the numbers of above finite sequence of numbers to their equivalent letters in the alphabet, the original plaintext (message) "TEACHERS" is reproduced.

4. Conclusions

Complex SEE integral transform is proved to be a promising new integral transform that could be exploit in cryptography field, and as a capable integral transform, it used successfully to perform encryption on a plaintext and transform it into unintelligible ciphertext, then inverse

SEE integral transform is succussed to retrieved the original ciphertext from the received ciphertext.

References

[1] Christof Paar , Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 2010th Edition Springer-Verlag Berlin Heidelberg, 2010.

[2] Eman A. Mansour, Sadiq A. Mehdi, Emad A. Kuffi, The new integral transform and its applications, Int. J. Nonlinear Anal. Appl. (12) (2021) No.2.

[3] Eman A. Mansour, Sadiq A. Mehdi, Emad A. Kuffi, On the Complex SEE Change and Systems of Ordinary Differential Equations, International Journal of Nonlinear Analysis and Applications (12) (2) (2021).

[4] Eman A. Mansour, Sadiq A. Mehdi, Emad A. Kuffi, Application of New Transform "Complex SEE Transform" to Partial Differential Equations, Journal of Physics: Conference Series, Vol. 1999, No.1, 2021.

[5] Eman A. Mansour,Emad A. Kuffi, Sadiq A. Mehdi, Complex SEE Transform of Bessel's Functions, Journal of Physics: Conference Series, Vol. 1999, No.1, 2021.

[6] Emad A. Kuffi, Ali Hassan Mohammed, Ameer Qassim Made, Elaf Sabah Abbas, Applied al-Zughair transform on nuclear physics, International Journal of Engineering & Technology, Vol.9, No.1, (2020), pp. 9-11.

[7] Elaf Sabah Abbas, Emad Kuffi, Sara Faleh Maktoof Alkhozai, Solving improved heat transmission measuring equation using partial differential equations with variable coefficients, International Journal of Engineering and Technology, Vol. (7), No. (4), (2018) 5258-5260.

[8] P. Senthil Kumer, S. Vasuki, An application of Mahgoub Transform in Cryptography, Advances in Theoretical and Applied Mathematics, Vol.(13), No.(2), (2018).

[9] Hemant K. Undegaonkar, R.N.Ingle, Role of Some Integral Transforms in Cryptography, International Journal of Engineering and Advanced Technology, Vol.(9), (2020).

[10] V. Srinivas and C.H. Jayanthi, Application of the New Integral "J-

transform" in Cryptography, International Journal of Emerging Technologies Vol. (11), No. (2), (2020).