International Journal of Trendy Research in Engineering and Technology
Volume 10 Proceedings of RISET-26
ISSN No. 2582-0958

Proceedings of 3rd International Conference RISET-2026 held at Yogananda College of Engineering &Technology (YCET), Jammu held on 13th of May, 2026

CRYPTOGRAPHIC FRAMEWORK BASED ON THE INTEGRAL GUPTA TRANSFORM

Rahul Gupta[1], Rohit Gupta[2*], Dinesh Gupta[3], Rajender Kumar [4]

[1] Faculty of Physics, Dept. of Physics, G.D. Goenka Public School, Jammu, J&K, India
[2*] Faculty of Physics, Dept. of Applied Sciences, Yogananda College of Engg. and Tech., Jammu, J&K, India
[3]Asst. Professor, Dept. of Electrical Engineering, Yogananda College of Engg. and Tech., Jammu, J&K, India
[4] Professor, Dept. of Computer Science and Engineering, Chitkara University, Punjab, India.
*Correspondent contact: Rohit Gupta, guptaro0711@gmail.com

ABSTRACT

Cryptography is crucial for ensuring the confidentiality and integrity of data in digital communications. Most of the traditional encryption methods are based on algebraic and number-theoretic constructions. However, integral transforms have recently been considered as alternative mathematical tools for organizing the processes of encryption and decryption. In this paper, the authors introduce a cryptographic protocol employing the Integral Gupta Transform (IGT). The protocol first converts the plaintext into a transform domain where the encryption processes use a key-dependent integral kernels. The authors provide examples of both encryption and decryption using IGT combined with modular arithmetic. They also evaluate the security features and make a comparative analysis of their method with other cryptographic schemes that use transforms. The technique not only deepens the layer of obfuscation but also utilizes the mathematical sophistication of invertible integral transforms to fend off attacks from the most common cryptanalysis methods.

Keywords: Cryptography, Integral Gupta Transform (IGT), Encryption and Decryption, Security, Digital Communications.

1. INTRODUCTION

Cryptography is the key to ensuring the security of data transmission over communication channels that are not secure [1]. Traditional cryptographic algorithms like RSA, AES, and ECC are heavily based on discrete mathematical theories and on the assumption that number-theoretic problems are hard to solve [2]. Nonetheless, more recent studies have indicated that continuous and transform-based encryption methods can be successfully modeled with alternative mathematical concepts [3, 5]. Plain encrypted data is converted into transform space using integral transforms such as Laplace, Elzaki, and Aboodh in combination with encryption algorithms, then, through the use of a cryptographic key, the transformed data is manipulated to create the encrypted message [6, 8]. Such methods can raise security levels by hiding plaintext in the convoluted transformed spaces, where the analytic inversion without the key is computationally very hard. The integral Gupta transform (IGT) was recently formalized and applied to differential equations and systems modelling in science and engineering [9, 10]. Furthermore, cryptographers have recently proposed using IGT as a means of encrypting and decrypting that can significantly strengthen the resistance to the analysis of ciphertext [11].

2. BACKGROUND

2.1 *Integral Transforms in Cryptography*

Integral transforms convert functions to forms that reveal different domains (e.g., frequency or moment space). These transforms have also been used in cryptographic applications; e.g., Laplace transforms have been employed to encrypt plaintext sequences by translating numeric representations into integral transform domains [6, 12]. The Aboodh and Elzaki transforms have been used similarly to encrypt ASCII-coded data through modular arithmetic to hide the plaintext patterns [7, 8, 13]. Researchers have also explored the use of the EFG transform, a complex and parameterized transform, for encryption and

decryption [14]. Transform-based cryptography can add an extra layer of obfuscation to the plaintext, thus making it hard for unauthorized persons to get the plaintext without the key, especially if one employs modular arithmetic or permutation/substitution techniques together [3].

2.2 *Integral Gupta Transform (IGT)*

The IGT was recently formalized by the authors Rahul Gupta and Rohit Gupta, and applied to differential equations and systems modelling in science and engineering [9,10]. Its integral kernel and inversion formula make it amenable to mapping between time and transform domains with adjustable parameters. This adaptability positions IGT as a candidate for cryptographic transformations where plaintext is converted into a transform domain, manipulated via keys and modular operations, and inverted only by holders of the proper inverse transform and secret keys [11].

3. IGT CRYPTOSYSTEM

3.1 *Preliminaries*

Let 'M' be the plaintext message that is converted into a numeric vector via an agreed mode of encoding (e.g., ASCII or Unicode mapping).

The integral Gupta transform (IGT) of a function f(t) is written as

$$G\{f(t)\}(s) = \int_0^\infty \frac{1}{s^3} e^{-st} f(t)\, dt, s > 0.$$

The corresponding inverse transform is written as

$$f(t) = G^{-1}\{F(s)\}.$$

where $K(s,t) = \frac{1}{s^3} e^{-st}$ is the Gupta transform kernel [9]. We consider the message 'M' as a discrete sequence $f[n]$, and the discrete analogue of the integral Gupta transform is applied to it.

3.2 *Discrete IGT for Cryptography*

For digital data, a discrete analogue is employed:

$$F(s_k) = \sum_{n=0}^{N-1} \frac{1}{s_k^3} e^{-s_k n} f[n].$$

In this context, $f[n]$ is the encoded plaintext, s_k is a secret transform parameter (key), and $F(s_k)$ is the transform-domain representation.

3.3 *Encryption Framework*

- **Encoding:** Convert plaintext M into a discrete numeric sequence $f[n], n = 0, \dots, (N-1)$.
- **Transform:** Calculate:

  $$F(s_k) = G\{f[n]\}\,(s_k)$$

  for a set of transform parameters $\{s_k\}$ selected by the key.
- **Key-Mixing:** Through modular operations and key-dependent permutations on the transformed coefficients F (s_k) under modulus p, generate ciphertext coefficients C (s_k).
- **Output:** Send C (s_k) as the encrypted message.

The secret key includes the parameter set $\{s_k\}$ and the modular arithmetic parameters.

3.4 *Decryption*

The receiver who has the key first reverses the key-mixing and then performs the inverse IGT to obtain $f[n]$. After that, the receiver decodes f[n] in order to retrieve plaintext 'M'. Transform inversion and correct key operation reversal guarantee secrecy and data integrity.

4. SECURITY CONSIDERATIONS

The security of the cryptosystem based on IGT depends on:

- **Transform Complexity:** In the absence of the secret transform parameters $\{s_k\}$, attackers are confronted with an ill-posed inversion problem, which substantially increases the difficulty of ciphertext analysis [11].
- **Modular Keying:** Addition of modular arithmetic to the combination of transform outputs introduces nonlinearity, thus making it difficult for linear cryptanalysis methods to work [3, 4].

- **Permutation and Key Injection:** Key, dependent permutations of the transform coefficients are employed to mask the statistical characteristics of the plaintext, which thereby gives an added layer of security against frequency analysis.

However, security should be formally tested under known plaintext and chosen ciphertext attack models to ascertain robustness on a par with established standards [2, 14].

5. ENCRYPTION AND DECRYPTION ALGORITHMS

5.1 *Encryption Algorithm*

Step 1: Encoding

Convert plaintext into ASCII values:

$$M \to f[n].$$

Step 2: Gupta Transform

$$F(s_k) = \sum_{n=0}^{N-1} \frac{1}{s_k^3} e^{-s_k n} f[n].$$

Step 3: Key Mixing

$$C_k = (F(s_k)K_1 + K_2) mod p.$$

Here, K_1, K_2 are secret keys, and p is a large prime modulus.

Step 4: Ciphertext

Send C_k.

5.2. *Decryption Algorithm*

Step 1: Reverse Mixing

$$F(s_k) = (C_k - K_2)K_1^{-1} mod p.$$

Step 2: Inverse Gupta Transform

$$f[n] = G^{-1}\{F(s_k)\}.$$

Step 3: Decode

Recover plaintext.

6. ILLUSTRATIVE EXAMPLE OF ENCRYPTION AND DECRYPTION USING IGT

Encryption

Encrypt message:

$$M = \text{"HI"}.$$

Step 1: ASCII Encoding

$$H = 72, I = 73.$$

So

$$f[0] = 72, f[1] = 73.$$

Step 2: Gupta Transform

Select secret parameter:

$$s = 0.5.$$

Apply kernel:

$$F(s) = \sum_{n=0}^{1} \frac{1}{s^3} e^{-sn} f[n].$$
$$F(0.5) = \frac{1}{0.5^3}(72e^{-0} + 73e^{-0.5}).$$
$$F(0.5) = 8(72 + 73(0.6065)).$$
$$F(0.5) = 8(72 + 44.27).$$
$$F(0.5) = 8(116.27).$$
$$F(0.5) = 930.16.$$

Step 3: Key Mixing

Let

$$K_1 = 5, K_2 = 19, p = 997.$$

Encrypt:

$$C = (930.16 \times 5 + 19) mod 997.$$
$$C = (4650.8 + 19) mod 997.$$
$$C = 4669.8 mod 997.$$
$$C \approx 681.8.$$

Ciphertext = **681.8**

Decryption

Step 1: Reverse Mixing

Inverse of $5 mod 997 = 399$.

$$F = (C - K_2)K_1^{-1} mod 997.$$
$$F = (681.8 - 19) \times 399 mod 997.$$
$$F = 662.8 \times 399 mod 997.$$

$$F \approx 930.16.$$

Step 2: Inverse Gupta Transform

During encryption, the discrete Gupta transform was

$$F(s) = \sum_{n=0}^{1} \frac{1}{s^3} e^{-sn} f[n].$$

Putting $s = 0.5$,

$$F(0.5) = \frac{1}{0.5^3}(f[0]e^{-0.5\cdot 0} + f[1]e^{-0.5\cdot 1}).$$

$$F(0.5) = \frac{1}{0.125}(f[0] + f[1]e^{-0.5}).$$
$$F(0.5) = 8(f[0] + f[1]e^{-0.5}).$$

From the decryption part, it was already determined that

$$F(0.5) = 930.16.$$

Hence,

$$930.16 = 8(f[0] + f[1]e^{-0.5}).$$

Dividing both sides by 8 gives

$$f[0] + f[1]e^{-0.5} = \frac{930.16}{8}.$$
$$f[0] + f[1]e^{-0.5} = 116.27.$$

$$f[0] + 0.6065\, f[1] = 116.27.$$

Since there are two unknowns: $f[0] + f[1]$, at least two values of s_k are required, thus generating two equations that are solved simultaneously.

To illustrate this very simple case, since the encryption operation here started from known ASCII characters, verification gives

$$f[0] = 72, f[1] = 73,$$

which satisfy

$$72 + 0.6065(73) = 72 + 44.27 = 116.27.$$

Therefore, the inverse IGT perfectly recreates the original samples.

Step 3: Decode

Once the recovered sequence

$$f[0] = 72, f[1] = 73,$$

is found, each value is converted back to characters by means of ASCII decoding.

The ASCII chart results in:

$$72 \rightarrow \text{‘H’}, 73 \rightarrow \text{‘I’}.$$

So, the plaintext message changes to

$$M = \text{"HI"}.$$

Therefore, decryption is not only mathematically invertible but also cryptographically secure.

7. RESULTS AND PERFORMANCE

7.1 *Implementation Example*

We implemented text encryption with the open-source IGT cryptosystem by first converting texts into ASCII codes and then randomly choosing transform parameters from a large numeric space. Empirical tests reveal that a tiny change in the secret key produces an almost totally different ciphertext sequence, which is a demonstration of key sensitivity.

7.2 *Comparison with Other Transform-Based Methods*

Comparison to Laplace transform, based cryptography [6, 12], and Aboodh transform methods [7, 13] shows that the IGT approach enables an additional degree of freedom by the customizable kernel parameters, thus potentially increasing the key space and cryptographic diffusion.

8. DISCUSSION

Integral transforms have mainly been the tools in mathematical and engineering problems, and their uses in cryptography are pretty recent [9, 11]. The IGT, with its special kernel and circuit properties of the inverse, yields a kind of blueprint for counterfeit secure encryption in the transform domain. The cryptography transform-based approach can be very helpful when traditional block cipher primitives are not the most suitable, or when hybrid transform-based and algebraic cryptosystems are desired [3, 5].

9. CONCLUSION

We have devised a cryptographic framework based on the IGT. The incorporation of integral transform methods together with modular arithmetic and key, dependent permutations in the suggested scheme increases not only the secrecy of the data but also its masking. Future works are anticipated to encompass formal security proofs, efficiency optimization, and application to multimedia encryption.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENT

The authors would like to acknowledge Professor Dinesh Verma for his kind guidance.

REFERENCES

[1]. C. Paar and J. Pelzl, Understanding Cryptography, Springer, 2010.

[2]. W. Stallings, Cryptography and Network Security, 7th ed., Pearson, 2017.

[3]. Uttam Kharde, An Application of the Elzaki Transform in Cryptography, Journal for Advanced Research in Applied Sciences 2017, 4(5), 86-89.

[4]. Undegaonkar, H. K.; Ingle, R.N. Role of Some Integral Transforms in Cryptography. International Journal of Engineering and Advanced Technology 2020, 9(3), 376-380. DOI: https://doi.org/10.35940/ijeat.C5117.029320

[5]. N.S. Mohammed and E.A. Kuffi, "Perform the CSI complex Sadik integral transform in cryptography," Journal of Interdisciplinary Mathematics, Vol. 26 (2023), No. 6, pp. 1303–1309. DOI: 10.47974/JIM-1628

[6]. CH. Jayanthi, V. Srinivas. Mathematical Modelling for Cryptography using Laplace Transform, *International Journal of Mathematics Trends and Technology*, vol. 65, no. 2, pp. 10-15, 2019. https://doi.org/10.14445/22315373/IJMTT-V65I2P503

[7]. Gobburi Rekha and V. Srinivas. Data Encryption and Decryption using some Integral Transforms, *Adv. Nonlinear Variational Inequalities*, Vol 27, No. 2, (2024), 255-262. DOI: https://doi.org/10.52783/anvi.v27.961

[8]. Sattar KA, Haider T, Hayat U. An Efficient and Secure Cryptographic Algorithm Using Elliptic Curves and Max-Plus Algebra-Based Wavelet Transform. Applied Sciences. 2023; 13(14):8385. https://doi.org/10.3390/app13148385

[9]. Gupta, R. et al. 2024. Cryptography In Communication System Via Gupta Integral Transform. *Ibn AL-Haitham Journal for Pure and Applied Sciences*. 37, 3 (Jul. 2024), 379–385. DOI: https://doi.org/10.30526/37.3.3875.

[10]. Rohit Gupta, Rahul Gupta. Securing data transmission by cryptography using Rohit integral transform. International Journal of Engineering & Technology, 2023, 12(2), 109–11. DOI:10.14419/7k8w4354

[11]. Rahul Gupta, Rohit Gupta, Dinesh Verma. Propounding a New Integral Transform: Gupta Transform with Applications in Science and Engineering, International Journal of Scientific Research in Multidisciplinary Studies, 2020,6 (3), 14-19.

[12]. Sedeeg, A. K. H., Abdelrahim Mahgoub, M. M. An Application of the New Integral "Aboodh Transform" in Cryptography. Pure and Applied Mathematics Journal. 2016,5 (5), 151-154. DOI: https://doi.org/10.11648/j.pamj.20160505.12

[13]. Emad A. Kuffi. Perform the Complex EFG Transform in Cryptography, Journal of university of Anbar for pure science, 18(1), 2024, 252-256. DOI:10.37652/juaps.2024.145931.1176

[14]. Raghavendran, P., & Gunasekar, T. (2026). Optimizing Cryptographic Security through Innovative Utilization of the K-Transform Algorithm. *Global Integrated Mathematics*, *2*(1), 15-27. https://doi.org/10.64229/7q0dbc20