25th International Scientific Conference UNITECH

INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025
GABROVO

ИМПЛЕМЕНТИРАНЕ НА ХИПЕРХАОТИЧНА СИНХРОНИЗАЦИОННА СХЕМА В АЛГОРИТЪМ ЗА КРИПТИРАНЕ НА ИЗОБРАЖЕНИЯ БАЗИРАН НА ФРАКТАЛНО ТРОМИНО

Христина Стойчева

Технически университет – Габрово, България
Кореспондиращ автор: hsstoycheva@tugab.bg

IMPLEMENTATION OF HYPERCHAOTIC SYNCHRONIZATION SCHEME IN IMAGE ENCRYPTION ALGORITHM BASED ON FRACTAL TROMINO

Hristina Stoycheva

Technical University of Gabrovo, Bulgaria
Corresponding author: hsstoycheva@tugab.bg

Abstract
This paper considers the possibility of implementing a hyperchaotic synchronization scheme in an image encryption algorithm. A chaotic synchronization scheme between two hyperchaotic Singh-Row systems based on the second Lyapunov stability method is used. By transforming the chaotic signal, the possibility of implementing the synchronization scheme in a communication image encryption system using an algorithm based on a fractal tromino is provided. The implementation is done in a Matlab/Simulink environment, and the results are presented graphically.
Keywords: image encryption, chaos, fractals, secure communication.

ВЪВЕДЕНИЕ

Бързото развитие на комуникационните технологии и широкото използване на цифрови изображения в различни области – от интернет комуникации [1,2] до медицинска диагностика [3,4] – налагат необходимостта от надеждни методи за защита на визуална информация. Традиционните криптографски алгоритми като AES [5] и RSA [6] осигуряват високо ниво на защита, но тяхната ефективност може да бъде ограничена при обработка на големи по размер изображения или при приложения в реално време. В тази връзка, нараства интересът към хаотичните и хиперхаотичните системи, които предлагат висока чувствителност към начални условия и псевдослучайност - свойства, изключително подходящи за изграждане на криптографски системи [7].

Използването на хаотична синхронизация в комуникационни системи позволява надеждно възстановяване на хаотичния сигнал в приемника, което я прави особено подходяща за приложения в областта на сигурното предаване и декодиране на информация. Прилагането на хиперхаотични системи — системи с повече от един положителен показател на Ляпунов — допълнително повишава степента на защита, благодарение на по-

Print ISSN: 1313-230X, Online ISSN: 3033-1404

сложната им динамика и многомерното им поведение.

В настоящата работа се разглежда имплементирането на хиперхаотична синхронизационна схема в алгоритъм за криптиране на изображения, базиран на фрактално Tromino. Синтезираната синхронизационна схема е реализирана между две хиперхаотични системи на Singh–Roy, като управлението е синтезирано по втория метод за устойчивост на Ляпунов. Хаотичният сигнал, получен от синхронизацията, се използва в различните етапи на алгоритъма за криптиране – от генериране на ключовете до финалната трансформация на изображението.

ИЗЛОЖЕНИЕ

Представената техника за кодиране на изображения се основава на комбинация на известен алгоритъм базиран на фрактални функции [8] с хаотичен сигнал. За реализиране на декодирането е необходима хаотична синхронизация с цел получаване на използвания за кодирането хаотичен сигнал.

Хиперхаотична система и синхронизационна схема

Синтезирана е хаотична синхронизационна схема между две идентични хиперхаотични системи на Singh – Roy [9] с комбиниран вид синхронизация, съчетаващ три основни вида хаотична синхронизация, а именно хибридна, мащабирана и изместена [10].

Системата на Singh – Roy, е абстрактен математичен модел, базиран на системата на Liu-Chen и се описва със следните уравнения:

$$\begin{aligned}\dot{x}_1 &= -x_2 - x_3 - ax_4,\\ \dot{x}_2 &= x_1,\\ \dot{x}_3 &= b(1 - x_2^2) - cx_3,\\ \dot{x}_4 &= dx_1.\end{aligned} \quad (1)$$

Оптималните стойности на параметрите за които в системата възникват хаотични колебания са $a = 1.378, b = 0.5, c = 0.6$ и $d = 0.097$.

Синхронизационната схема е от типа Master - Slave с управляваща система (1) и подчинена система:

$$\begin{aligned}\dot{\tilde{x}}_1 &= -\tilde{x}_2 - \tilde{x}_3 - a\tilde{x}_4 + u_1,\\ \dot{\tilde{x}}_2 &= \tilde{x}_1 + u_2,\\ \dot{\tilde{x}}_3 &= b(1 - \tilde{x}_2^2) - c\tilde{x}_3 + u_3,\\ \dot{\tilde{x}}_4 &= d\tilde{x}_1 + u_4.\end{aligned} \quad (2)$$

За постигане на комбинираният метод за синхронизация е необходимо към подчинената система да се прибави не само управляваща функция, а и съответните коефициенти на мащабиране α_i, както и коефициентите на изместване c_i. В този случай системата от разсъгласуването между двете системи придобива следния обобщен вид:

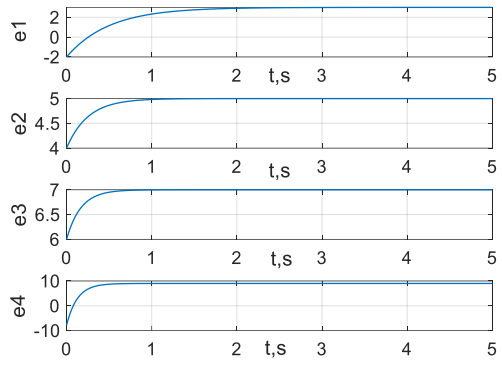
$$\dot{e}_i(t) = \mathbf{f}(\mathbf{x}) \pm \alpha_i \mathbf{f}(\tilde{\mathbf{x}}) \pm \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}) + c_i \quad (3)$$

където $\mathbf{f}(\mathbf{x})$ и $\mathbf{f}(\tilde{\mathbf{x}})$ са нелинейни функции, а $\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}})$ е управляващ сигнал към системата (2). Началните условия на системата са различни, т.е. $\mathbf{x}(0) \neq \tilde{\mathbf{x}}(0)$.

С цел постигането на надеждна синхронизация на база втори метод за устойчивост на Ляпунов са синтезирани следните управляващи функции:

$$\begin{aligned}u_1 &= \frac{-x_2 - x_3 - ax_4 + \alpha_1\tilde{x}_2 + \alpha_1\tilde{x}_3 + a\alpha_1\tilde{x}_4}{\alpha_1} - c_1 + k_1 e_1,\\ u_2 &= \frac{-x_1 - \alpha_2\tilde{x}_1}{\alpha_2} + c_2 - k_2 e_2,\\ u_3 &= \frac{-b + bx_2^2 + ce_3 - \alpha_3 b + b\alpha_3\tilde{x}_2^2}{\alpha_3} + c_3 - k_3 e_3,\\ u_4 &= \frac{dx_1 - d\alpha_4\tilde{x}_1}{\alpha_4} - c_4 + k_4 e_4.\end{aligned} \quad (4)$$

Началните условия на управляващата система са $\mathbf{x} = [0\ 0\ 0\ 0.1]^T$, а на подчинената система – $\tilde{\mathbf{x}} = [1\ 1\ 1\ 1]^T$, като и двата набора са избрани произволно. Коефициентите на изместване и мащабиране също са избрани произволно както следва: $\alpha_1 = 2$, $\alpha_2 = 4$, $\alpha_3 = 6$, $\alpha_4 = 8$, $c_1 = 3$, $c_2 = 5$, $c_3 = 7$ и $c_4 = 9$.



***Фиг. 1**. Функции на разсъгласуване*

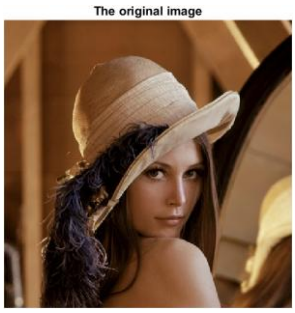
На фиг. 1 са представени получените функции на разсъгласуване, които графично потвърждават настъпването на режим на комбинирана хаотична синхронизация преди втората секунда от преходния процес.

Кодираща процедура

Най-общо алгоритъмът се състои от четири модула: генериране на ключ, фрактално кодиране, хаотично кодиране и декодиране. В разглежданата модификация, хаотичния сигнал се използва във всеки един от модулите, започвайки от генерирането на ключа, който за разлика от традиционният алгоритъм, тук се изчислява многократно в зависимост от големината на изображението. На практика направената модификация увеличава степента на защита многократно, а използваният хаотичен сигнал, присъства на всички нива от кодировката, включително и в процеса на генериране на фракталното Tromino. От друга страна, хаосът се използва и във финалния кодиращ алгоритъм, като DCT (discrete cosine transform), след което се получава финалното кодирано изображение. Респективно, кодираното изображение се декодира, чрез обратно прилагане на хаотично базираният модул и фрактално базираният декриптиращ алгоритъм. Използваният хаотичен сигнал в процеса на декриптиране, се получава след процес на синхронизация.

Кодиращата процедура може да се представи в следните стъпки:

1. *Представяне на входното изображение* – Получава се матрична интерпретация на входното изображение, като се изчисляват неговите размери (редове и колони) и брой пиксели.

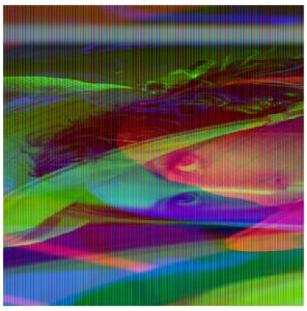


***Фиг. 2**. Входно изображение*

2. *Транспониране на фракталите* – избира се и се инициализира размера на фрактала и фракталната кодираща матрица, който може да бъде обвързан с входното изображение. Най-общо, на тази стъпка се разделят трите цветови канала на входното изображение, образуват се три нови изображения за всеки от каналите и се транспонират. Така получените три изображения, отново се сливат в едно. Процеса по трансформация е представен на фиг 3 и фиг. 4.

а) Red б) Green в) Blue

***Фиг. 3**. Новообразувани изображения за всеки от цветовите канали*



***Фиг. 4**. Полученото след процеса по трансформация общо изображение*

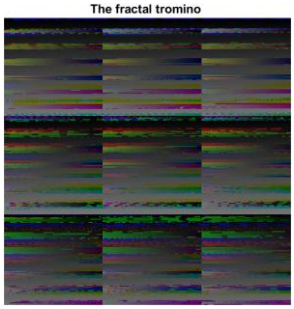
3. *Подготвяне на L формите на фракталното tromino* – това отново е инициализираща стъпка, при която се избират началните условия, като начална локация във фракталното изображение, резолюция и начало на изчисляване на фрактала.

4. *Фрактален модул за кодиране* – Най-общо фракталният модул за кодиране може да се раздели на две фази:

- *Фаза 1* – формиране на ключове и фаза 2 - оформяна на фракталното tromino. Фаза 1 и фаза 2 участват в итерационен цикъл, който се повтаря $3nm$ пъти, където n и m оказват размера на входното изображение. Ключовете за изчисляват по формулите (5) и (6):

$$key1 = 5x_{1m} * x_{3m} + 4 \quad (5)$$

$$key\,2 = x_{2m} * key1 \quad (6)$$

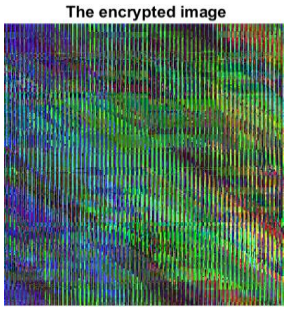


***Фиг. 5**. Кодиращо изображение*

- *Фаза 2* – Във втора фаза се оформя формата на фракталното tromino посредством разделяне на по-малки tromino-та от същия тип. Процеса също е итерационен, като образуването на формата се базира на две променливи $\theta = 90°$ и L приемащ „+“ или „–“ стойности. На фиг. 5 е показано генерираното кодиращо изображение.

5. *Кодиране на изображението* – на този етап се осъществява същинското кодиране на входното изображение, чрез използване на XOR (Exclusive OR) операцията с вече генерираното кодиращо изображение. Този тип алгоритъм зависи от модулни операции и поради тази причина е напълно обратим. Поради това си свойство той представлява едно към едно криптиращ-декриптиращ алгоритъм, т.е. входното изображение не може да бъде повредено по време на декриптирането.

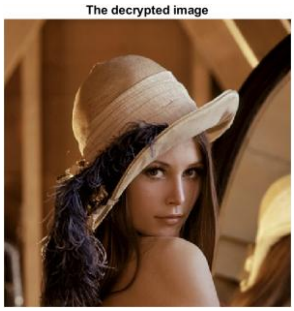
Примерно кодирано изображение е показано на фиг.6.



***Фиг. 6**. Кодирано изображение*

6. *Декриптиране на изображението* – след като процесът на криптиране е приключил, декриптирането се явява обратна процедура по извличане на оригиналното изображение. При този метод декриптирането се извършва по същите стъпки като при процедурата на кодиране, с тази разлика, че вече входното изображение се явява кодираното. Преди изпълняване на началните стъпки се използва избраната синхронизационна схема с цел получаване в приемника на същият хаотичен сигнал използван за генериране на кодиращото изображение. Тъй като при синхронизация на хаотичните системи е налице преходен процес, то за избягването му се въвежда параметър, даващ времезакъснение при използването на хаотичния сигнал, както при коди-

рането, така и при декодирането. Това допълнително покачва степента на защита, тъй като се предоставят възможности за избиране на хаотични трендове от хаотичния сигнал. На фиг.7 е показано декодираното изображение.

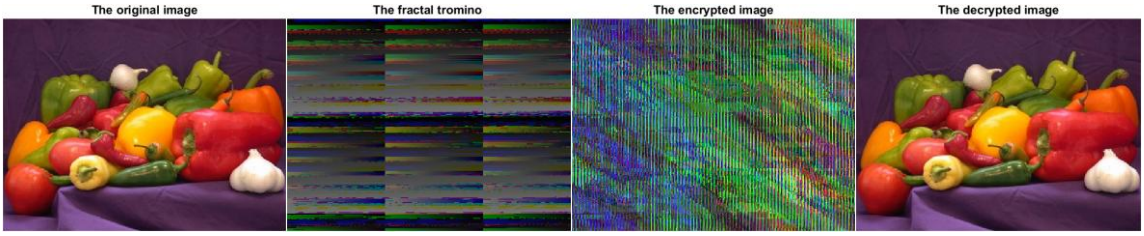


Фиг. *7. Декодирано изображение*

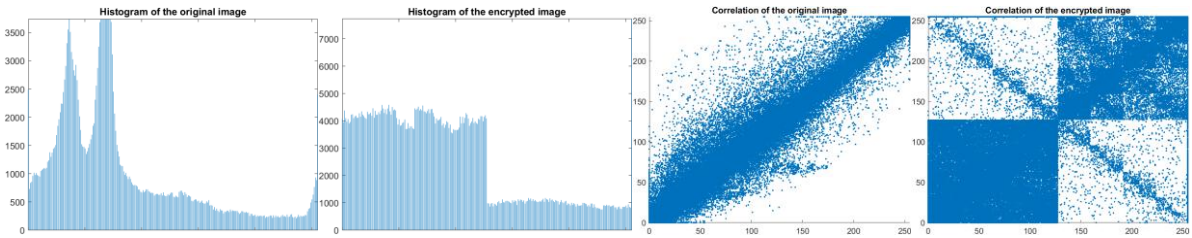
Процесът по имплементиране на хиперхаотична синхронизационна схема в алгоритъм за криптиране на изображения базиран на фрактално тромино е приложен за четири стандартни тестови изображения.

Всяко от избраните тестови изображения е крипритано и декриптирано, като са изведени графичните интерпретации на хистограмите и корелационните изображения на изследваните изображения. На фиг.8 е графично представен процеса по кодиране на изображението „Peppers“. Хистограмите и коралационните изображения за същото изображение за представени на фиг. 9. Изведени са същите графични интерпретации за изображение „Pout“ (фиг. 10 и фиг.11) и изображение „Baboon“ (фиг. 12 и фиг.13).

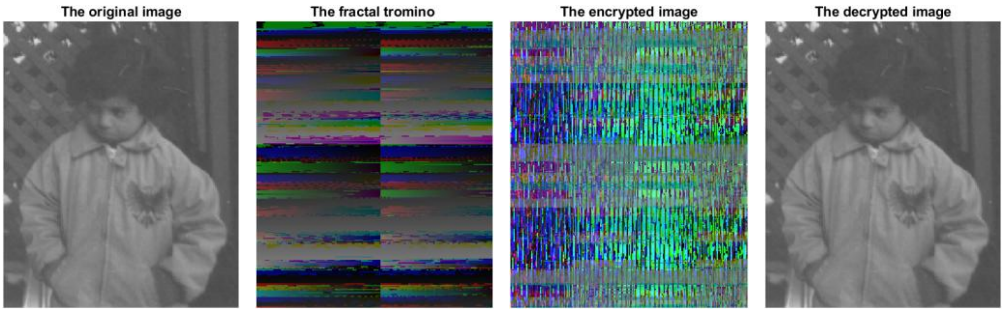
Графични резултати



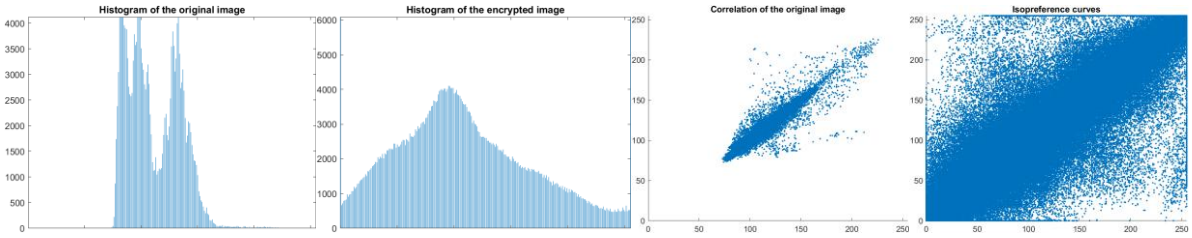
Фиг. 8*. Криптиране на изображение “Peppers”*



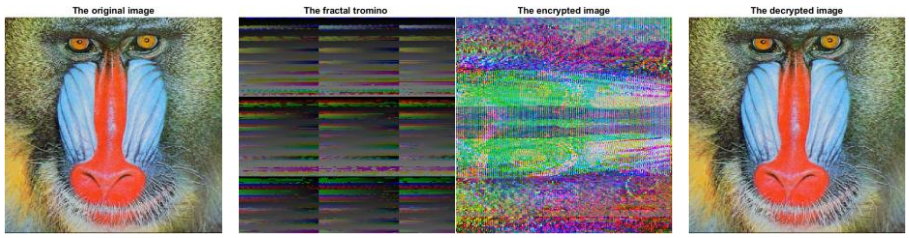
Фиг. 9*. Хистограми и корелационни изображения за оригинално и кодирано изображение “Peppers”*



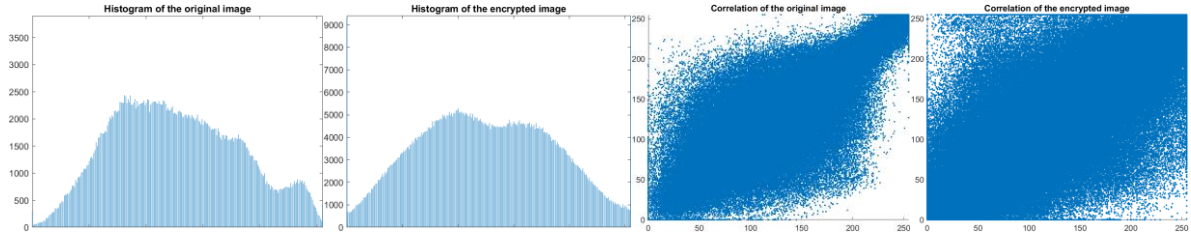
Фиг. 10*. Криптиране на изображение “Pout”*



***Фиг. 11**. Хистограми и корелационни изображения за оригинално и кодирано изображение "Pout"*



***Фиг. 12**. Криптиране на изображение "Baboon"*



***Фиг. 13**. Хистограми и корелационни изображения за оригинално и кодирано изображение "Baboon"*

Числови резултати

Представените графичните интерпретации на хистограми и корелационни характеристики могат да се използват за визуален анализ и първоначално определяне на степента на защита на информацията. От изведените изображения, могат да се получат числови резултати, които дават конкретен отговор без субективна преценка за постигнатото ниво на защита.

В таблица 5.1 са показани стойностите на информационната ентропия за тестовите и съответните криптирани изображения.

***Таблица 5.1** Числови резултати за информационната ентропия*

Изображение	оригинално	кодирано	декодирано
Lena	7.3283	7.6762	7.3283
Peppers	7.0692	7.7006	7.0692
Pout	6.2156	7.7545	6.2156
Baboon	7.6634	7.8250	7.6634

В таблица 5.2 са показани стойностите на корелацията между пикселите на тестовите изображения и съответните криптирани изображения.

***Таблица 5.2** Числови резултати за корелацията на изследваните изображения*

Изображение	оригинално	кодирано	декодирано
Lena	0.9811	0.8810	0.9811
Peppers	0.9826	0.8342	0.9826
Pout	0.9796	0.8842	0.9796
Baboon	0.8191	0.7671	0.8191

Получените числови резултати потвърждават високата ефективност на предложената криптографска схема. Стойностите на информационната ентропия за всички криптирани изображения са близки до теоретичния максимум от 8, което показва равномерно разпределение на стойностите на пикселите и липса на статистическа зависимост в кодираното изображение. Едновременно с това, из-

числените коефициенти на корелация между оригиналните и криптираните изображения са значително по-ниски (в диапазона 0.76–0.88) в сравнение с тези на оригиналните изображения, което показва ефективно разрушаване на взаимовръзките между съседни пиксели. Ниската корелация и високата ентропия потвърждават, че предложената комбинация между хиперхаотична синхронизация и фрактален Tromino алгоритъм осигурява надеждно криптиране с висока устойчивост срещу статистически и корелационни атаки.

ЗАКЛЮЧЕНИЕ

В настоящата работа е представен метод за имплементиране на хиперхаотична синхронизационна схема в алгоритъм за криптиране на изображения, базиран на фрактално Tromino. Резултатите от симулациите потвърждават надеждната работа на синхронизационната схема и успешното постигане на комбинирана хаотична синхронизация в кратък преходен процес. Числовите и графичните анализи показват висока стойност на информационната ентропия и ниски корелационни коефициенти между оригиналните и криптираните изображения, което свидетелства за равномерно разпределение на пикселите и ефективно разрушаване на зависимостите между тях. Това доказва, че предложената система осигурява високо ниво на сигурност и устойчивост срещу статистически атаки.

Този доклад и изследванията в него са реализирани по проект „Съвременни методи и AI решения за защитено предаване на данни в широколентови комуникационни мрежи“, договор НИП 2025-14/2025 г. към УЦНИТ при ТУ – Габрово.

ЛИТЕРАТУРА

[1] Jain, K., Titus, B., Krishnan, P., Sudevan, S., Prabu, P., & Alluhaidan, A. S. (2024). A lightweight multi-chaos-based image encryption Scheme for IoT Networks. IEEE access, 12, 62118-62148.

[2] Zhong, Y., Lai, Q., Zhu, C., & Qin, M. (2025). A new multi-image encryption scheme for Smart Home IoT integrating hyperchaos and compressive sensing. Computer Standards & Interfaces, 104051.

[3] Lai, Q., & Hua, H. (2025). Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes. Expert Systems with Applications, 264, 125854.

[4] Razaq, A., Maghrabi, L. A., Ahmad, M., Aslam, F., & Feng, W. (2024). Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine. Ieee Access, 12, 7584-7608.

[5] Hadj Brahim, A., Ali Pacha, A., & Hadj Said, N. (2024). An image encryption scheme based on a modified AES algorithm by using a variable S-box. Journal of Optics, 53(2), 1170-1185.

[6] Ullah, S., Liu, X., Waheed, A., & Zhang, S. (2025). S-box using fractional-order 4D hyperchaotic system and its application to RSA cryptosystem-based color image encryption. Computer Standards & Interfaces, 93, 103980.

[7] Alghamdi, Y., & Munir, A. (2024). Image encryption algorithms: a survey of design and evaluation metrics. Journal of Cybersecurity and Privacy, 4(1), 126-152.

[1] Pramudya, E. R., Soeleman, M. A., Jatmoko, C., Rachmawanto, E. H., Marjuni, A., Andono, P. N., & Isinkaye, F. O. (2024). Optimation of image encryption using fractal Tromino and polynomial Chebyshev based on chaotic matrix. TELKOMNIKA (Telecommunication Computing Electronics and Control), 22(6), 1529-1540.

[9] Singh J. P., ROY B. K., A novel hyperchaotic system with stable and unstable line of equilibria and sigma shaped poincare map, IFAC-PapersOnLine, 2016, 49.1: p. 526-531.

[10] Stoycheva, H., & Chantov, D. (2020, October). Design of chaotic synchronization system combining projective, marginal and hybrid synchronization with application to image encryption. In 2020 International Conference Automatics and Informatics (ICAI) (pp. 1-6). IEEE.