Indian Journal of Artificial Intelligence and Neural Networking (IJAINN)
ISSN: 2582-7626 (Online), Volume-1 Issue-3, June 2021

A Hybrid Visual Cryptography Method using Sigmoid Function for Security Enhancement in Gray Scale Images

Dinesh Kumar, Kailash Patidar, Gourav Saxena, Rishi Kushwaha

Abstract: ***Visual encryption technology becomes the latest research area in which a lot of scopes persist. Presently such a particular cryptosystem procedure is now used by numerous other countries around the world for the private transmission of formal records, financial documents, content visuals, digital voting, and so on. Visualization Cryptographic algorithms one of the protected methods of transferring pictures online. The main benefit of image encryption has been that it disguises peripheral vision with encrypt data secret data with no computation usually needed. In this work a hybrid visual cryptography method using a sigmoid function (HVMSF) for enhancing the security in gray images. HVMSF strategy utilizes a chaos framework to scramble pixel values as well as blocks while using the Modified Arnold Cat Map method (MACM) as well as the Henon Map method (HMM). The methodology includes a confusion procedure wherein the location of each image pixel is shuffled by utilizing MACM. The shuffling of image pixel leads to the creation of a subset pixel which will be protected for transmitting. This proposed HVMSF mainly tries to overcome the limitation of the previous approaches by applying sigmoid function in image feature space for contrast enhancement throughout the consequent source images. The experimental outcomes precisely show that the suggested strategy can further give additional effectiveness to ensure the protection of transmitting information out over previous techniques.***

Keywords: Visual Cryptography, Modified Arnold Cat Map (MACM), Henon Map (HM), hybrid visual cryptography method using a sigmoid function (HVMSF)

I. INTRODUCTION

Cryptography is the art and science of thrashing secret information in a broadcast network. The philosophy of a cryptography method is to conceal a large amount of covert data in a substantial host image, such that the rooted underground information is obstructed and illegitimate persons are prevented from attacking it. One way to protect multimedia data against unauthorized recording and retransmission is to provide a signal known as a digital signature, rights tag, or watermark that validates the information's owner [1,2]. Cryptography seeks to create a more advanced encryption program with just a significant number of and effective methods literature. In authentication, the three most significant targets are growing secret potential capacity, preventing threats, and increasing level of security. Cryptography is the capacity to secure messages wrapped in a medium such as audio, image, video, or text documents [3].

Throughout the research article, a cryptographic method based on GA was proposed HVMSF that secured RSA threats. This procedure inserts hidden bits into the cover image in the first phase, just like a basic LSB, and then reconfigures pixel strategies to make the steno model RS variables sit in the protected area in the final phase. The complete paper is divided into various sections, which cover the basics of visual cryptography, its existing methods, challenges, and applications in various domains. The next section of the research covers related work, proposed HVMSF model, and experimental setup and result in analysis, and finally covers conclusions and future work.

II. RELATED WORK

In this paper [4], the author has invented a new approach based on a genetic algorithm and tunable graphic image excellence and knowledge lossless methodology in the spatial domain (GA). The most important recommendation made by that technique is to show the difficulties of Steganography as an analysis and optimization problem.In the research paper [5] the process for inserting consists of two main steps: first, they change top-secret bits, and then they inject them into the host image. The arrangement of scanning host pixels and the opening location of scanning, as well as the most excellent LSBs of each pixel, are distinguished by swarming images in odd locations.

In the research article [6] a novel Steganography technique has gotten a demonstration on the request of wavelet convert and genetic procedure (GA). They attempt to make effort accessible for a GA-based mapping function to insert details in discrete wavelet transform (DWT) coefficients in 4 * 4 blocks on the enfold image in this article.

Manuscript received on April 03, 2021.
Revised Manuscript received on May 21, 2021.
Manuscript published on June 10, 2021.
* Correspondence Author
Dinesh Kumar*,M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore(Madhya Pradesh), India. Email: dineshkr.04@gmail.com
Kailash Patidar, Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, (Madhya Pradesh), India. Email: kailsashpatidar123@gmail.com
Mr. Gourav Saxena, Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, (Madhya Pradesh), India. Email: gauravsss1999@gmail.com
Mr. Rishi Kushwaha, Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, (Madhya Pradesh), India. Email:rishisinghkushwah@gmail.com

Following the message's insertion, the optimal pixel modification procedure (OPAP) is useful.In the research article [7] there are plans to develop a modern morphed steganography technique.

In general, image protection is a challenging issue nowadays. So, for thrashing clandestine knowledge in cover medium, the author employs the Steganography technique. The Least Significant Bit is a popular Steganography method with several limitations.

In the research [8] the standard steganography of data hiding in popular digital images has been studied. A new approach for increasing the capability of data hiding and the picture unnoticeable after adding the top-secret message is included in this proposed scheme. Often helpful to minimize the error discrepancy between the wrap and stego image is the suggested work, Optimal Pixel adjustment procedure.In the research [9] a modern Steganography strategy that embeds hidden messages in the frequency domain to give you an indication of whether the PSNR is still unmoving an appropriate evaluation when the uppermost competence situation is useful by giving the appearance of being at the results of replication. This is due to the DWT coefficients.

In the research [10] a new approach for picture Steganography based on DWT was demonstrated by the researcher. This document demonstrates a modern Copy Steganography technique based on DWT, in which DWT is used to change the original image, i.e. the cover image, from the spatial domain to the frequency domain. In the research [11] DEGGA is a GA-based algorithm. The key emphasis of this phase is on a vast volume of secret data, and the results are measured using a separate methodology. Using 3 x 3 masks from the source image, the Mandal technique inserts a large number of messages/images in the spatial domain.

III. VISUAL CRYPTOGRAPHY & METHODS, CHALLENGES

Visual cryptography seems to be an encryption method that enables visual data (images, messages, etc.) to have been encoded in just such a way that perhaps the decoded results indicate mostly as a visual object. A few of the best-known methods were recognized as "Moni Naor and Adi Shamir", which formed that in 1994 [12]. Steganography approaches can be exploited by two groups of people: those in the Image Domain and those in the Transform Coefficients. The image also known as 'spatial domain' methods specifically insert signals in the intensity of the pixels, while translate is also known as ‘frequency domain’ methods change the image first then correct the signal in the picture. Around all types of files could be included in the mainframe image Steganography, but images were proven to be the most complete aspect of the embedding due to their high level of joblessness. When we analyze, discuss, and extend steganography techniques, three considerations [13-16] must be considered:

- **Capability:** switch to the sum of data that can interleave to the swathe reflection, which was called payload for a moment [17].
- **Resilience:** conflicts with various compressed image processing.
- **Safety:** reducing the changes in the envelope illustration to fight steganalysis and HVS with the influence of the stego symbol.

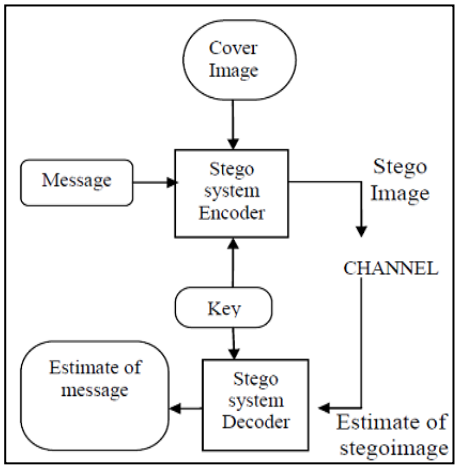


Figure 1.1 Traditional Image encryption (cryptographic) structures [18]

1.1 Visual cryptography methods- Following methods are widely used in visual cryptography [19]-

1.1.1 Image steganography domains- Steganography itself received significant and ongoing research support from researchers all over the world. As a result of these recommendations from the research community, a large number of inserting approaches have been proposed, some of which have been useful for gray-scale images and others for colored images [20].

1.1.2 Spatial domain embedding-Space Domain an objective pose of the constituent in an image supports steganography. Encoding is involved at the LSB level. Only the LSB wrap thing is restored without the whole wrap. It is the simplest technique to insert data but is fragile in counterattacks like compression and alterations.

1.1.3 Transform domain embedding- Since the document morsels are loosely coupled straight to the image pixel sections, LSB embedding strategies are the safest way to interleave the furtive sense keen on the swath, but as discussed, they are highly vulnerable to stegano-analysis identification.

- ***Discrete Cosine Transformation (DCT):***It is virtually universally revered in the transform domain because the DCT pedestal figure layout (JPEG) is widely used and is the most common digital camera production [21].
- ***Discrete Wavelet Transformation (DWT):*** The traditional strategies of embedding using LSB are still functional, but the difference is to the top furtive, suggesting that fragments can be loosely coupled into the wavelet coefficient bits (LSB) instead of moving bits of actual pixel pieces.
- ***Integer Wavelet Transformation (IWT):*** This methodology retains the wavelet coefficients' stability even at well beyond the opinion expertise adding, which was achieved by approximating the capability of each DWT block and applying the embedding procedure to the whole block rather than the bit-planes [22].

3.2 Challenges in existing methods- The existing methods have the following challenges [23]-

- **Poor Contrast ratio:** The existing method encounters with low contrast pictures can result in Deterioration illumination, absence of dynamic range.
- **Peak Signal to Noise Ratio (PSNR):** PSNR stands for the proportion of a signal's greatest available power to the power of influencing noise, which impacts the consistency of its recognition. The existing method generates a lower PSNR value.
- **Mean-Signal-to-noise ratio (MSNR)**: Higher MSNR shows a better image quality. The existing method [1] shows a poor value for MSNR.
- **Mean Squared Error (MSE):** The variance between input images and a reference image is measured by MSE. The MSE with a lower value shows a promising outcome. The existing methods have an average value for MSE.
- **Normalized Absolute Error (NAE):** It is mainly used to measure the image quality. The existing method generates an average value for NAE. Lower the NAE value shows better image quality.

IV. OBJECTIVE &PROPOSED HVMSF METHOD

In this work a hybrid visual cryptography method using the sigmoid function (HVMSF) for enhancing the security in gray images. HVMSF strategy utilizes a chaos framework to scramble pixel values as well as blocks while using the Modified Arnold Cat Map method (MACM) as well as the Henon Map method (HMM) [26].

4.1Objective- The main objective of the proposed HVMSF method is as follows:

- To improve the contrast.
- To improve the PSNR result.
- To improve the MSNR results.
- To improve the MSE results.
- To improve the NAE results.

4.2 Proposed HVMSF methodology- In this work a hybrid visual cryptography method using the sigmoid function (HVMSF) for enhancing the security in gray images. The methodology includes a confusion procedure wherein the location of each image pixel is shuffled by utilizing MACM. The shuffling of image pixel leads to the creation of a subset pixel which will be protected for transmitting. This proposed HVMSF mainly tries to overcome the limitation of the previous approaches by applying sigmoid function in image feature space for contrast enhancement throughout the consequent source images.

Proposed HVMSF algorithm

Step1 - Sij pixel is the input called the original pixel with the position I and j.
Step2 - Sij' = 255 – Sij (Pixel problem smear).
Step3 - To decrease Si I' haphazardly use quasi accidental quantity manufacturer (0.1 to 0.9).
Step4 - Take Sij's change by innovative Sij pixel.
Step5 - Reduce Sij's overturned charge erratically using a quasi-haphazard quantity producer.
Step6 - Setback for smear pixels, i.e.Sij = 255 – Sij
Step7 - As an image, segment 1 is a stockpile in the environment.
Step8 - Consider the addition of two inventive pixel S ij to two chance figure producers.
Step9 -Setback for smear pixels, i.e.Sij = 255 - Sij.
Step10 - Save Sij''' as a split 2 image in the medium
Step 11 -Both portion 1 and share 2 should be heaped.
Step 12 -Apply the sigmoid mask to every pixel.
Step 13 -The final encrypted image is displayed.

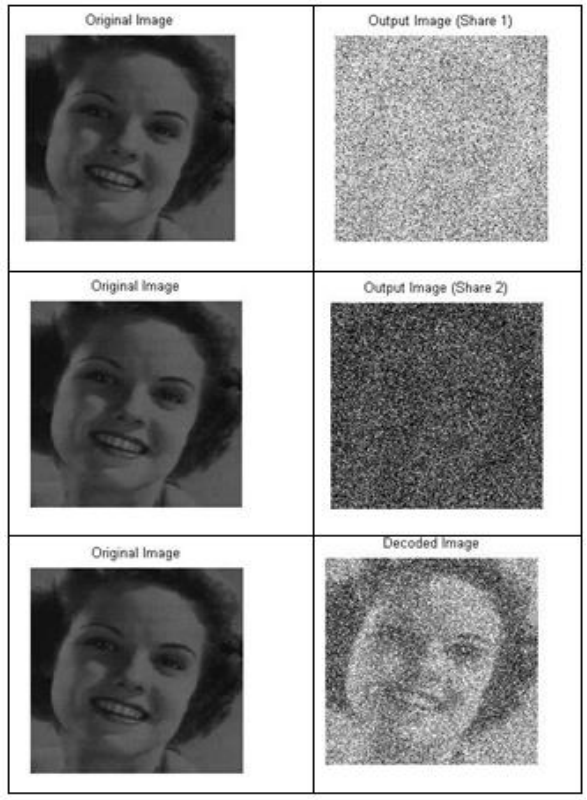
V. EXPERIMENTAL RESULTS & ANALYSIS

The proposed HVMSF method and the existing method [1] both are implemented in a MATLAB Simulation.

5.1Comparison Parameters- Following performance measuring, parameters were calculated-

- **Image Contrast ratio:** A higher contrast picture can result in a better quality of an image.
- **Peak Signal to Noise Ratio (PSNR):** PSNR stands for the proportion of a signal's greatest available power to the power of influencing noise, which impacts the consistency of its recognition.
- **Mean-Signal-to-noise ratio (MSNR)**: The difference between a processed image and a reference image is measured by MSE. The MSE with a lower value represents a better result.
- **Normalized Absolute Error (NAE):** It is mainly used to measure the image quality. Lower the NAE value shows better image quality.

5.2 Simulation Results- Various images were used in these experiments, one of which was a 512*512 image. Each portion of Share 1 and Portion 2 was 512*512 pixels.



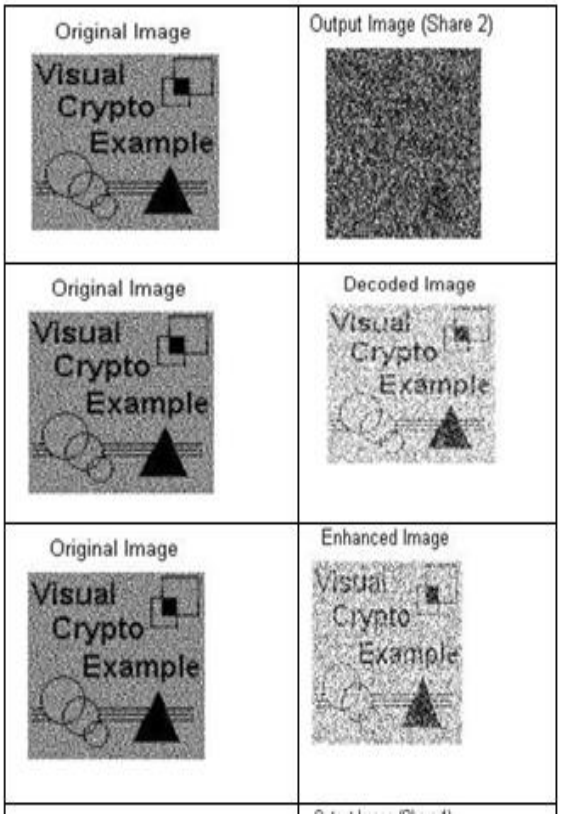


Figure 1.2 Simulation Result for existing [1] and proposed method

The underground image will be molded as shown in the figure above by loading Share 1 and Share 2 composed.

Table 1.1 Simulation Results for existing [1] and proposed HVMSF method for various images

Image	Method	Contrast Ratio %	PSNR %	MSNR %	NAE %
image-1	Existing [1]	37.78	32.54	19.23	0.3789
	Proposed HVMSF	41.51	35.89	18.44	0.0298
image-2	Existing [1]	41.22	31.9	21.56	0.381
	Proposed HVMSF	47.5%	36.78	17.99	0.0217
image-3	Existing [1]	38.69	32.56	23.33	0.398
	Proposed HVMSF	46.5%	38.92	19.22	0.0278
image-4	Existing [1]	39.96	30.56	20.22	0.372
	Proposed HVMSF	45.68	34.97	18.54	0.0289

The experimental result for the existing [1] and proposed HVMSF method in table 1.1 is clearly showing that the proposed method has a better result image contrast ratio %, PSNR %, MSNR %, and NAE %, for image 1 to image-4.

VI. CONCLUSION & FUTURE WORK

Visual cryptography is indeed the prevailing field of studies in which the majority of scope continues to exist. Currently, this accurate cryptographic structure seems to be emergence used mostly by various parts of the world for secretively transmitting typewritten catalogs, economic booklets, phone cameras, vote counting, etc. Visual Cryptography produces another of the shielded behaves to transmitting images or videos over the internet with safety.

In this research work, a hybrid visual cryptography method introduced, using the sigmoid function (HVMSF) for enhancing the security in gray images. HVMSF strategy utilizes a chaos framework to scramble pixel values as well as blocks while using the Modified Arnold Cat Map method (MACM) as well as the Henon Map method (HMM). The image accompanying is very readable and productive in dealing with poor pictures. The image is very well created. The simulation results clearly show that the proposed method has better result image contrast ratio %, PSNR %, MSNR %, and NAE %, for image 1 to image-4. In future work, we can use the proposed strategy to evaluate the experimentation performance for color pictures.

REFERENCES

1. X. Yan, F. Liu, W. Q. Yan, G. Yang, and Y. Lu, 'Weighted visual cryptographic scheme with improved image quality, *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 21345–21360, 2020.
2. P. Anghelescu, I.-M. Ionescu, and M. B. Bodea, 'Design and implementation of a visual cryptography application', in *2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2020.
3. X. Yan, F. Liu, W. Q. Yan, and Y. Lu, 'Applying visual cryptography to enhance text captchas', *Mathematics*, vol. 8, no. 3, p. 332, 2020.

4. Y.-W. Ti, S.-K. Chen, and W.-C. Wu, 'A new visual cryptography-based QR code system for medication administration', *Mob. Inf. Syst.*, vol. 2020, pp. 1–10, 2020.
5. R. Maurya, A. K. Kannojiya, and B. Rajitha, 'An extended visual cryptography technique for medical image security, in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2020.
6. Kumar and A. Jain, 'A review on various implemented techniques for visual cryptography', *Int. J. Comput. Appl.*, vol. 155, no. 5, pp. 27–32, 2016.
7. S. Dutta, A. Adhikari, and S. Ruj, 'Maximal contrast color visual secret sharing schemes, *Des. Codes Cryptogr.*, vol. 87, no. 7, pp. 1699–1711, 2019.
8. Y. Wang, Y. Li, and X.-N. Lu, 'Evaluation criteria for visual cryptography schemes via neural networks, in *2020 International Conference on Cyberworlds (CW)*, 2020.
9. M. Melkemi and K. Hammoudi, 'Voronoi-based image representation applied to binary visual cryptography', *Signal Process. Image Commun.*, vol. 87, no. 115913, p. 115913, 2020.
10. Adhikari, 'Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images', *Des. Codes Cryptogr.*, vol. 73, no. 3, pp. 865–895, 2014.
11. H. Koga and T. Ishihara, 'A general method for construction of (t, n)-threshold visual secret sharing schemes for color images', *Des. Codes Cryptogr.*, vol. 61, no. 2, pp. 223–249, 2011.
12. S. Kukreja, G. Kasana, and S. S. Kasana, 'Extended visual cryptography-based copyright protection scheme for multiple images and owners using LBP–SURF descriptors', *Vis. Comput.*, 2020.
13. P. Li, J. Ma, and Q. Ma, '(t, k, n) XOR-based visual cryptography scheme with essential shadows', *J. Vis. Commun. Image Represent.*, vol. 72, no. 102911, p. 102911, 2020.
14. X. Wu and C.-N. Yang, 'Probabilistic color visual cryptography schemes for black and white secret images', *J. Vis. Commun. Image Represent.*, vol. 70, no. 102793, p. 102793, 2020.
15. K. Gupta, S. K. Sadana, and B. Gupta, 'Geospatial data preprocessing and visualization for the logistics industry', *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 1, pp. 57–64, 2020.
16. M. E. VizcarraMelgar and M. C. Q. Farias, 'A (2,2) XOR-based visual cryptography scheme without pixel expansion', *J. Vis. Commun. Image Represent.*, vol. 63, no. 102592, p. 102592, 2019.
17. X. Wu, D. Chen, C.-N. Yang, and Y.-Y. Yang, 'A (k,n) threshold partial reversible AMBTC-based visual cryptography using one reference image', *J. Vis. Commun. Image Represent.*, vol. 59, pp. 550–562, 2019.
18. C.-N. Yang, F.-H. Wu, and S.-L. Peng, 'Enhancing multi-factor cheating prevention in visual cryptography based minimum (k, n)-connected graph', *J. Vis. Commun. Image Represent.* vol. 55, pp. 660–676, 2018.
19. S. Sridhar and G. F. Sudha, 'Two in One Image Secret Sharing Scheme (TiOISSS) for extended progressive visual cryptography using simple modular arithmetic operations', *J. Vis. Commun. Image Represent.*, vol. 74, no. 102996, p. 102996, 2021.
20. X. Wu and C.-N. Yang, 'A combination of color-black-and-white visual cryptography and polynomial based secret image sharing', *J. Vis. Commun. Image Represent.*, vol. 61, pp. 74–84, 2019.
21. N. Ren, L. Fan, and Z. Zhang, 'Sensorless PMSM control with sliding mode observer-based on sigmoid function', *J. Electr. Eng. Technol.*, 2021.
22. Y. Zhang, X. Luo, J. Wang, Y. Guo, and F. Liu, 'Image robust adaptive steganography adapted to lossy channels in open social networks', Inf. Sci. (NY), vol. 564, pp. 306–326, 2021.
23. L. Zhu, X. Luo, C. Yang, Y. Zhang, and F. Liu, 'Invariances of JPEG-quantized DCT coefficients and their application in robust image steganography', Signal Processing, vol. 183, no. 108015, p. 108015, 2021.
24. T. Qiao, S. Wang, X. Luo, and Z. Zhu, 'Robust steganography resisting JPEG compression by improving the selection of cover element', Signal Processing, vol. 183, no. 108048, p. 108048, 2021.
25. K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, 'Multi-directional block-based PVD and modulus function image steganography to avoid FOBP and IEP', J. Inf. Security. Appl., vol. 58, no. 102808, p. 102808, 2021.
26. G. Gambhir and J. K. Mandal, 'Shared memory implementation and performance analysis of LSB steganography based on chaotic tent map', Innov. Syst. Softw. Eng., 2021.
27. S. Dash, Kalinga Institute of Industrial Technology, M. Das, D. Behera, Kalinga Institute of Industrial Technology, and Silicon Institute of Technology, 'An improved dual steganography model using multi-pass encryption and quotient value differencing', Int. j. intell. eng. syst., vol. 14, no. 2, pp. 262–270, 2021.

AUTHOR PROFILE

Dinesh Kumar, is pursuing M.Tech CSE from School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India. His research area includes machine learning, data analysis and security.

Kailash Patidar,is currently working as an Assistant Professor in Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India. His research area includes machine learning; cloud computing, data analysis and security.

Rishi Kushwaha,is currently working as an Assistant Professor in Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India. His research area includes machine learning; cloud computing, data analysis and security.