Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 1, January 2021: 419-428

Implementing Visual Cryptographic Scheme Based Cipher Technique: A Review

Abhishek Garg[1] and Kishan Pal Singh[2]
[1]Department of Computer Engineering & Applications, Mangalayatan University, Aligarh, UP
[2]Department of Mechanical Engineering, Mangalayatan University, Aligarh, UP
Corresponding Authors Email: - [1]abhishek47722@gmail.com, [2]kishan.singh@mangalayatan.edu.in

ABSTRACT:
The Internet is a fast-growing communication system and an essential part of infrastructure today. Dealing with the growth of the Internet has become an ongoing struggle to protect the privacy and protect data copyright when it comes to profits. Many steganographic methods are designed to ensure the confidentiality and copyright of data. But each process has its advantages and disadvantages. If one approachcannot load, the other does not have compatibility. Therefore, the main emphasis of cryptography is to overcome these errors.A 2-by-2 vcs security classification structure was developed to withstand network attacks for transmitting fingerprints. In this paper, the standard meaning of vcs is the visual cryptographic scheme. Reconstructing the hidden image using 2 out of 2 distributed vcs shares is lost compared to the re-created image. Many private photos can be shared between n users using the k sharing via the k out-of-n vcs program. The only requirement is a small effort to move and distribute pixels between stocks. It has been argued that the digital watermark system is copyrighted, copyrighted image privacy and, data security. This database program cannot challenge existing steganography solutions for the same purpose, thus adding complexity to achieve the same goal. The author proposes a solution based on a bubbling overflow problem system to apply malicious code. The attacker is smart enough to write such sections using clever planning techniques. BASED ON THE GCC EDITOR, the MRAS solution customs a modified adaptive tool to conflict with the overcrowding delinquent.

Detective technique rather than block. It also writhes from environmental dependence. The generalprocedure of the Internet has led to the development of threats such as phishing scams, spam, and hijackings that could result in your account information being hacked by cybercriminals. Cyber instructions are set against all possible online crimes, but monitoring procedures are not easy enough for any ordinary victim. OTP confidential shares of account information are processed using cryptography encrypted and encrypted with quantum cryptography; this is easy and secure for e-commerce systems today. Generating time keys and sharing them safely on these breaks is a complex process, to begin with. Many private photos can be transmitted simultaneously using audio sharing on each n + 1. This system works much better than RSA-based VCS as it uses more straightforward module functionality than Boolean XOR. The proposed method uses n + 1 audio images for recreating custom images that upsurge space and time interval complexity. We can reduce the number of shares to make it more efficient than the current one. If custom images are of a different size, the projected system will not work.

KEYWORDS:
Cryptography, Steganography, Watermarking, Visual Image.

INTRODUCTION:

The Caesar Cipher method is one of the oldest and easiest ways to encrypt. It is a type of substitution cipher;a fixed number of lowercase letters replaces each letter of a given text. For example, with a change of 1, A will be replaced by B, B will be C, etc.There are different passwords based on foreign exchange strategies and conversions. However, they only apply to text data. The data sent through the communication channel between the two sides of the image have a definite requirement for encrypting image data. A simple system would be to split an image into pixels; encode the color of each pixel in bits. The palette's number of colors will determine the number of bytes received. Each pixel representing the color in the picture will be marked with a different bit pattern. The whole image will be divided into a matrix collection line for each pixel pattern. Two-pixel patterns adjacent to the corresponding area in the matrix collection can be added to XOR. The key to this cipher will be the rotation of the line and column in the matrix collection. As discussed above, the cipher is made up of the efficiency of adjacent pixel models of matrices. The real message will be generated by the same process of converting the appropriate matrix. The algorithm uses specific randomization techniques and their application.

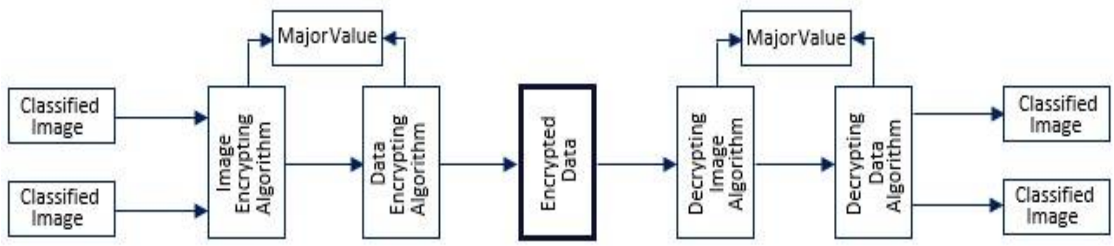

MajorValue
Classified Image
Classified Image
Image Encrypting Algorithm
Data Encrypting Algorithm
Encrypted Data
MajorValue
Decrypting Image Algorithm
Decrypting Data Algorithm
Classified Image
Classified Image

Figure 1: Visual cryptographical data management flow

Then, the next important article discusses security concerns in this cryptographic system. How can this algorithm increase the number of color combinations; thus, making the algorithm more complex. This algorithm will include XOR of more than two adjacent pixel patterns. It should make strong password attacks impossible. Furthermore, this system was compared with the existing encryption methods for text data and should also be separated from steganography. The concept can be stretched out and transformed into a game also.

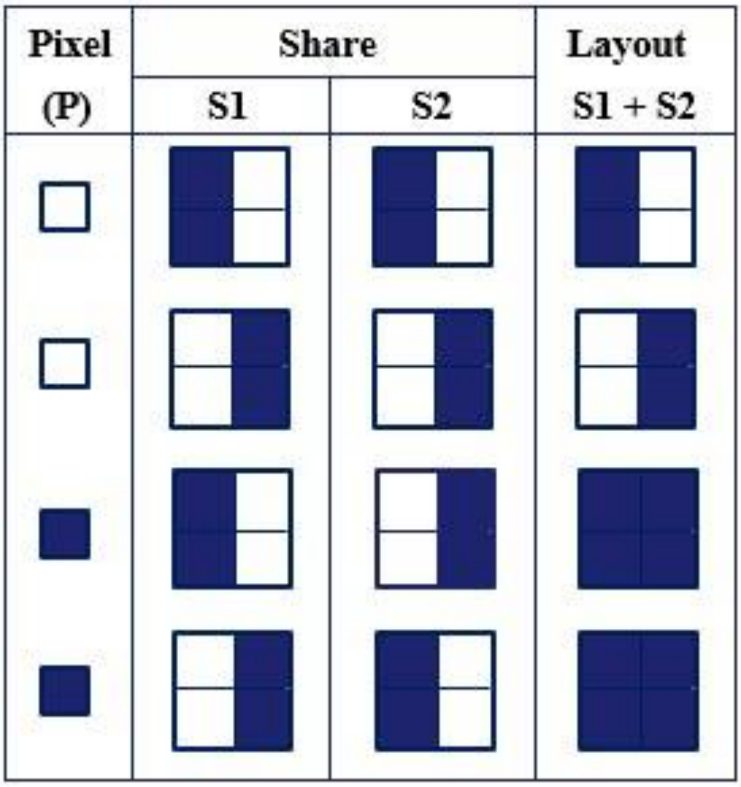
Because of encryption and recovery, it will do by splitting images into a few pictures posted via social media. The first image to function appropriately in these images requires a combination of previous cryptographic classifications and the appropriate integration into the current state; we can develop a plan that would be difficult for the attackers to destroy. The algorithm's complexity is handled in such anapproaching system that, on the one hand, it should be easy to encrypt the sender, and it should be easy and understandable to recruit recipients. On the other hand, it should be challenging to encrypt the analysis. They are hijackers.

VISUAL CRYPTOGRAPHY CLASSIFICATIONS:

Visual cryptography recommended by Naor and Shamir is one of the most secret ways to share personal photos. The visual cryptography of the Set P n participants is a method of encrypted (SI) encoding in shadow images, called stocks, in which each participant in P gets the task. Some small participants' 'fit sets' may circumvent SI, but others have no SI knowledge in the rejected sets of more minor participants. The 'visible rediscovery' of the appropriate X set means that they can detect SI by combining and packaging shares given to X participants in a public place. Thus, participants in the right X group will see SI without cryptography knowledge and cryptographic calculations.

VCS describes how an image is encrypted and how the encryption is removed. Various cryptography systems are emerging. For example, k-out-To encrypt an embodiment, the shares will be created, and the k-sharing must be stacked to clear the image encryption. If the number of stacked shares is less than k, the first image is not displayed. Other schemes are 2-n-out and n-out-n VCS. In the 2-out-of-n system, any dual sharing will be created and image encryption.

Table 1: The pixel pattern for 2-out-of-2-vcs with the layout


Pixel
(P)
Share
S1
S2
Layout
S1 + S2

Must tap to remove image encryption. In the n-out-of-n system, n sharing will be created for image encryption, and n-sharing should be matched to clear image encryption. If the number of stacked shares is less than n, the first image is not displayed. Increasing the number of shares or participants will automatically increase the security level of encrypted messages.

RELATED WORK:

(Thomas Monoth and Babu Anto P, 2010)developed a system for transmitting fingerprints using a secure channel using cryptography. The 2x2 VCS scheme algorithm was developed to send fingerprints with so many shares that kn participants needed to get the first image (kxnvcs scheme). Any number less than k will not cause a uniquephotograph.

(Hamada Ibrahim et al., 2012)IJCSI proposed a procedure in which multiple confidential images could be shared simultaneously between n users. The number of shares required for each SI will be the same as for the required (k, n) -VCS. And this does not need you to have more or more pixel extensions. Pixel extension here means that each post will be sent to all posts using a 2 or 3-pixel extension. Only pixels need to be directed and distributed intelligently enough for each task. This strategy does not affect existing systems' security, including skincare sharing skins.

(D.Mathivadhani et al., 2012)proposed a set of stamping schemes using advanced image processing techniques and visual cryptography. 'Digital Watermark' is defined as invisible or audio data (random bit or audio pattern) permanently embedded in an image, video, or audio file to protect data, copyright or authentication. Multi-watermarking is defined as adding multiple watermarks to a cover image. Multiple stamping incorporates the benefits of a single stamp algorithm to create a sophisticated, efficient, and secure stamping scheme. Visual Encryption (VC) is an extended image-sharing program. It has the power to retrieve confidential data without using statistics. VC is used with a watermark in the current function to allow multiple watermarks to be embedded in the same image without editing the larger picture. The main goal of the current research project is to develop sophisticated stamping schemes with visual encryption to encrypt information, copyright protection, and certification. This study is divided into two sections to achieve the goal as mentioned above,

Stage 1: Recommend and upgrade your encryption watermark algorithm, copyright protection, and authentication and select a practical algorithm for each location.

Stage 2: Use the selected algorithm and develop multiple stamping schemes.

In Phase 1, four stamp schemes are proposed. The first method includes Visual Encryption and an advanced Least Significant Bit (LSB) method to create a robust and secure marking method. The modified KP-Gillies feature algorithm integrated with Visual Encryption is the second proposed single tag system. The third model combines continuous-wave conversion with single-digit distortion and visual cryptography. The fourth model combines an independent component analysis with a variation of a separate wavelet pack.

(Yan Fen et al., 2012) provided a solution to defend against buffer overflow attacks.

How is buffer overflow made?

```
        char func(char *str);
        {
Char buf[128];
        strcpy(buffer,str);
        do something (buffer);
        }
```

If the str is 136 bytes, the bathroom will overflow, and the contents of the str will be written over the stack frame indicator and the return address space. No strcpy test is present to see if str exceeds belt size. If it is full of fragments listed in the return address section, the system can be made very liquid or use malicious code. The attacker calculates how much money is left in the memory from the P system recovery address section and causes it to override the correct value in the return address section in str. to launch the P system, the shell extraction code.

Program P is created ("\ bin \ sh"). By using the P system, the user controls the shell. If the attacker finds any difficultycalculating the original address of Program P, add NOP slides to read Program P.

Combining each variable (list or identifier) + with a 32-bit random number and using xor encryption at the return address value can attack in vain. If the attacker tries to write the return address in C, he can victory. $C \oplus MaskA \oplus MaskB$ provided $MaskA \neq MaskB$.

Program P
NOP
NOP
Return address
Char buf[128]

Stack Frame

(Sahel Alouneh et al., 2013)described the protection of mass memory from repetitive and random actions. Each activity call in the system creates a stack space that will be provided to maintain its parameters, including the return address; At this point, you return to work when you are done. Suppose this return address is written over some malicious code due to overcrowding. It happens because no systematic tests were performed to cause overflow. Now the attacker takes control of the shell and can cause the whole application to crash. This problem can be solved with the help of a software solution called a patch tool. The tool creates multiple copies of recovery addresses and randomizes them, and they do their random offset within stack segments. And the number of copies and messages arranged; Therefore, Return of Stack Address (MRAS) and properties.The patch tool is designed to use over the GCC component. The installer is a virus file infected with an object dump disassembler and fragmented into a compatible x86 file. Call the source program file and generate MRAS in that file, which receives and protects against stack-based attacks on binary integration against the GCC coordinator. System performance is tested against factorial, Fibonacci, algorithm configuration, and the problem is adequately calculated to a lesser extent.

(Julian Jang et al., 2014)surveyed threats to Cyber Security. Various malware has had a significant impact on the way communication is used. Spam distributes junk mail in a user's mailbox, thus consuming mail space. 1: 12M purchase of pharmacy product or 1: 260K spam greeting card causes infection; this is a botnet storm. To track a user into clicking on an ad on a website could result in the theft of victim information, which is a phishing scam. Website vulnerability is a rich marketing tool in the industry or black markets. Phishing scams are used to trick javascript into web pages and trick you into redirecting them to a scam site using typos.

As an internet expert, there is a great need to implement security measures such as blocking a security system or IDS. These security systems are designed for hardware or software. Distributed DOS attacks are used as malware attacks. Another threat to users by email and harassment is cyberbullying. Cyber rules work against this, but the procedures to be followed are complicated for the average user, and due to ignorance, we are getting worse today in cybercrime.

(Shemin P A et al., 2016)developed an electronic payment system using Visual and Quantum Encryption. E-commerce is widely used today. Identity theft and theft of sensitive information is significant concern today. The customer secretly writes the account number and other credit card information and sends it to you as a private bank account. There is also one share on the bank's website. By combining the two shares, the actual card details are available. Account details are also embedded when the password is generated by quantum cryptography. It occurs to prevent stock theft and so-called cybercriminals. Still, OTP verifies the account details and shares created by virtual cryptography to control the information disclosed to the attacker. After obtaining OTP verification and accounting information using the session key generated in each transaction between the merchant and the bank, the bank transfers the wallet from the customer's account to the merchant's account. In this program, image steganography is used in post-work OTP embedding.

Two encryption schemes are used for visual imagery and quantum cryptography to protect customer data via pre-used OTP and disclose shared intimate images. This program prevents Man-in-the-Middle attacks. Image steganography prevents identity theft by embedding data after the encrypted message has been transmitted to a secure channel. The program also directs cybercrime.

(Mohit Rajput et al., 2016)developed a secure image sharing system (n, n + 1) using Additive Modulo Operation. Shared private image N. These are converted to n + 1 audio images with an encryption algorithm. Personal audio sharing is required to re-create actual n + 1; any number below can reproduce the secret. All shares are stored on separate servers. An additional random server key is required to encrypt each sharing. And this program is much more secure than an RSA-based privacy sharing system because of its more straightforward operation of the add-on module that is easier to integrate than Boolean XOR. The image is generated as a Random pixel matrix for each function. Each image encryption uses a different private key than the one you share.

(Joseph Gualdoni et al., 2017) Suggest purchasing Online Transaction using Two-factor Verification. Buying online with a credit card requires special attention today. Other scams are registered as a Nigerian invasion and a US lottery scam to get a personal ID card. Some sensitive card information, such as number, code, and expiration date, are printed themselves and can be stolen and misused by another person as a passing waiter. In addition to these phishing scams, other phishing scams on the website can be exploited so that the attacker can register as their authorized user and trick the user into accessing helpful information. 2-factor authentication can add security, which may require you to enter a username and password and a verification code without entering your credit card details. This code is generated by a smartphone connected to a user account to make matters worse for the attacker. Attempts to register a new device and connect to a new machine with a user account will prevent adding security. Today, attacks on social engineers have also turned violent. An example is checking Mati Aharoni's login to create a web link and previously used internet stamps to use her computer illegally by tricking and allowing that person to click on the link.

(KambizGhazinour et al., 2017)They have created a model to prevent sharing sensitive information on smartwatches. Wearable technology affects us in many areas of life. Smart-watches used today are popular because of their wide range of features. They can say no. number of steps, heart rate, calories burned, and distance traveled. They are using an app installed on a mobile device to sync your watch. They need authorization in the app to use the smartwatch. Smart-watch collects app data on mobile devices with built-in protection of the system. You can now control your mobile device by reporting your calls and locating your device.

(Abdalla WasefMarashdihZaaba et al., 2017)Describe the adverse effects of the web application style. An attacker can embed web pages or text created by himself. Lumberjack uses malicious code and enables the attacker to read access details in the web browser, enabling cookies. If your browser has JavaScript enabled, the attacker may refer to Java text on your website; this may cause the user to redirect to the website. The attack mentioned above ispersistent, but there is a constant attack when the attacker does not change the web site's content (or make permanent changes).The attacker gets essential information about the victims and probably increases the risk of exploitation and the website's integrityfor measuring complex user inclusion to repeated exploitation.

(Fayez Hussain Alqahtani et al., 2017) Sample research development policy. IT organizations share their knowledge with the media today. This data needs to be protected from physical attacks. Therefore, Organizations should focus on the issue of confidentiality, integrity, and confidentiality. It includes safeguarding organizational resources and protecting internal threats, not external threats. Internal threats, even those within the organization, have access rights but exercise their rights. External threats point to appropriate ways to secure such protective walls to protect the intranet. Relevant policies should be applied, and all users in the organization should adhere to these policies, and users who are unable to follow the same should be treated by the organization's security team. The main areas covered by these security guidelines (as set out in the policy document) are privacy management, email, Internet, Social Networking sites, photographic information, and laptops. The main problems mentioned in this scenario are not using a portable computer, sending fake emails, browsing attachments, using malicious websites, sharing illegal content online, browsing the Internet, or using data online. Or conversely, downloading uncontrolled content online, visiting SNS, following verification policies usually kills valuable time on the SNS during business hours, using mobile networks to monitor internet traffic, access business channels without organizations.

(Martin Harran et al., 2018)describes how to ensure the integrity and authenticity of digital media. Connect to digital jpeg files. These files are used to check authentication, integrity, and data file can be significant with digital information. In-file metadata includes the digital signature of the CA, namely Release; Verification of the issuance of a digital CA signature is done with separate software. These tools need to be adjusted to different machines or applications; he ran evenly on the platform. Digital certificates include jpeg metadata. Even if file data is changed, image data embedded in the heart of the image remains intact and digital certification is valid. A cryptographic hash containing metadata and written code of hash image compared to a digital conversion certificate if the data is not converted. But if the image hash data eventually agrees to be a digital certificate,the certificate is invalid. Digital certificates are still distributed through high-quality orders, and the CA issues digital certificates for the number of children published by the CA at that level. Five companies offer digital certifications to Comodo, Godaddy, GlobalSign, and Symantec. In Italy, the incident occurred when cybercriminals attacked a salesman; If yComodo blocks company certificates issued. There was another case in the Netherlands where a digital certificate was given to a customer. Still, the entire company revoked all its Digital credentials without the consent of the Dutch Council.

(A. Salama et al., 2018)describe how to protect unprotected images in a channel using an encryption key. The leading secret sharing is done with the defined Hellman Lists algorithm. This action is used in particular stocks. This sharing may be encrypted for password sharing. A vc threshold is employed in private shares, using the k of n shares. Two sets of restricted sets apply to one shareholder. When used under shared participants, confidentiality disclosure is shared or used in addition to supervising a shared collection. Another method that uses multiple secret shares is used where shares are created at levels where each pixel produces two claims at the next level. And there is another way to share editing that will be shared with the next round of the first part and unveil a secret image overlay.

(Anatoliy Kovalchuk et al., 2019) They have developed an effective encryption method with Grayscale color graphics.This article introduces an effective encryption and image encryption method using the RSA algorithm mixed with other clever functions to maximize the cryptographic power of the encryption method. Some noisy tasks add complexity to the encrypted imageto make the situation worse for the attacker. The process is detailed: The pixel intensity matrix is arranged sequentially from the image. RSA calculations are then calculated using specific statistical parameters, including image length, length, and hypothetical numbers. Deleting encryption is against this method. The process also improves the performance of the bit-per-pixel xor ever produced by RSA. The matrix is created due to coding and encrypting all information about the image. The embedded image is slightly dimmed but still looks like an actual image. This method is as essential as the previous methods of preventing unauthorized images - watermark copyright, cryptography, steganography, etc.

(ȘtefanNicula et al., 2019)have exploited a stack of bath-based baths using modern techniques. The overflow of the bath takes control of the system's operation by typing the return address of the stack frame, which occurs as a result of the surge caused by the failure to comply with the parameters of the same object. A possible solution is to add a functional canary/cookies stack that can be added after the component has written parts of the stack frame. When an attacker tries to write over stack frames, the canary's value is determined by recalculating; if it differs from the set value. There is another method called Data Execution Prevention (DEP) which gives different kill rights to work so that the attacker can control the work environment without increasing the rights of the actual user. Space Layout Randomization (ASLR) continues to move the frame stacks to prevent the attacker from taking control.

(Devendrasinh Vashi et al., 2019)It has proposed the Hybrid Approach to Attribute-Based Encryption to protect privacy with horizontally segregated data.DES is a fair system that takes less time to operate, while RSA is an equally secure security cryptosystem. Therefore, a method that combines both schemes is used.

(Zeinab El. Rewini et al., 2019)discussed cybersecurity challenges in automotive communications. Cars are now automatically powered by V2X technology (one-on-one cars). The upper control layer controls speed, steering, and brake control. In the following areas, Sybil provides false attacks, MITM attacks, listening, impersonation, time attacks, etc. There may be online attacks. The so-called attack occurs when an attacker on the same route transmits false information to other vehicles on the current path. Heavy traffic congestion, so they changed their course. Now the attacker is free to use the network method without traffic. Sybil Attack creates additional nodes in the vehicle network and attacker, network intake, and network bandwidth.

(Jyoti Tripathi et al., 2020) described advanced optical encryption. To date, virtual cryptography has proposed producing k (n, n) shares and accumulating them. Custom image contains only black and white pixels. The program comprises black and white photos. The concept is extended to color illustrations. In the advanced color scheme (k, n), each pixel of the hidden image is encrypted using two-color models: the RGB color model and the CMY color model. The 24-bit image map is coded using 3-bit sequences embedded in different colors, red, green, and blue, respectively. This program does not require additional encryption keys for security, but it does design shares so that it is difficult to retrieve a private image from sharing, even if they are known for listening. This article (2, 3) discusses a virtual encryption system that not only reduces the performance of (3, 3) partners by reducing the number of shares but also makes it more efficient by using less bandwidth.

Using the program (2, 3), Advanced Visual Encryption makes it easy to transfer the image securely and protect it without using any shorthand to embed the image in place of the cover. Because revealing the secret of easy sharing of a personal recording system requires a complex calculation.

Another advantage of this program is that it does not have a pixel extension when collecting black and white image stocks based on visual encryption.
(Gayatri S et al., 2020) examined 20 hazards, threats, and legal issues and their impact on Distributed Cloud Environment and mitigation. A lot of data is shared in the cloud today. The integrity and confidentiality of this data become critical issues. There are many threats, some severe enough to threaten to undermine the organization's assets. Cybercriminal hackers can be as dangerous as embedded web script pages, and invalid tags called XSS spoofing. One can deny fraud even when disclosed; digital verification and denial methods using public keys are enabled in the system to combat the exploitation of such risks. In case of data loss, tools like a scalpel and PhotoRec can recover data. Scalpel is integrated with both Linux and Windows platforms. PhotoRec works on all file systems and can recover data even if the media file system is corrupted or formatted. Microsoft's STRIDE model protects against threats from cloud data such as XSS threats, interference and denial, disclosure of information, DOS, or fraudulent user identity fraud. The theft of sensitive information can be accounted for through appropriate access control measures such as one-factor authentication, dual-factor authentication, and three-factor authentication. Continuous development threats (APTs) are cyberattacks that infiltrate and damage the computer infrastructure of selected companies that capture their data. It can be calculated with IDS. The IDS also works against criminals.

PROPOSED WORK:

A 2-by-2 vcs secure system was developed to withstand any network attacksto transmit fingerprints. 2 out of 2 re-create a custom image using distributed shares via the vcs system lose out compared to the redesigned image. Custom images can be shared between n users using the k sharing in the kout-of-n vcs system. The only requirement is a small effort to move and distribute pixels between assignments. Next, we suggest developing a visual cipher with process language such as C and event planning language like VB6.0. Analyze the password pattern with Quality, Brightness, Rotation Level, and the space required for use. Rebuilding a custom image should be easy to find as we write with the same code. The algorithm should slightly distort the image with the correct comparison obtained. Shares should have the same pixel extension. We then compared the above model with existing ciphers and developed an efficient and easy-to-use schema such as symmetric schemes. The system is as secure as RSA in securing private shares. The functional k-out-n VCS system requires the development of black and white images as an existing system for color images. Next, we discuss the impact of buffer loading, cyberattacks attacks, and other network attacks on a visually enhanced cipher that proposes independent platform systems solutions where needed.

REFERENCES:

[1] Thomas Monoth, Babu Anto P. ICEBT 2010.Procedia Computer Science 2 (2010) 143–148.

[2] Maged Hamada Ibrahim1IJCSI International Journal of Computer Science Issues, Vol. 9,Issue 5, No 1, September 2012.ISSN (Online): 1694-0814.

[3] D.Mathivadhani, A Thesis Submitted ToAvinashilingam Institute for Home science and Higher Education for Women, Coimbatore – 641 043.

[4] Yan Fen, Yuan Fuchao, Shen Xiaobing1, Yin Xinchun1, Mao Bing.2012 International Conference on Applied Physics and Industrial Engineering.Physics Procedia 24 (2012) 1757 – 1764.

[5]Sahel Alouneh1, Mazen Kharbutli2, Rana AlQurem2The 4th International Conference on Emerging Ubiquitous Systems and Pervasive

Networks (EUSPN-2013). Procedia Computer Science 21 (2013) 250 – 256.
[6] JulianJang-Jaccard,SuryaNepal. Journal of Computer and System Sciences 80 (2014) 973–993.
[7]Shemin P A,Prof.Vipinkumar K S. International Conference on Emerging Trends in Engineering, Science and Technology, (ICETEST - 2015). Procedia Technology 24 (2016) 1623 – 1628.
[8] Mohit Rajput and Maroti Deshmukh.Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016). Procedia Computer Science 89 (2016) 677 – 683.
[9] Joseph Gualdoni, Andrew Kurtz, IlvaMyzyri, Megan Wheeler, and Syed Rizvi. Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS October 30 – November 1, 2017, Chicago, Illinois, USA Procedia Computer Science 114 (2017) 93–99.
[10] Kambiz Ghazinour1*, Emil Shirima, Vijayasimha Reddy Parne, Abhilash BhoomReddy.The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017).Procedia Computer Science 113 (2017) 105–112.
[11] Abdalla WasefMarashdih and ZarulFitriZaaba. 4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia.Procedia Computer Science 124 (2017) 647–655.
[12] Fayez Hussain Alqahtani. 4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia. Procedia Computer Science 124 (2017) 691–697.
[13] Martin Harran, William Farrelly, Kevin Curran. Applied Computing and Informatics 14 (2018) 145–158.
[14] May A. Salama, Mona F.M. Mursi, Manal Aly.Ain Shams Engineering Journal 9 (2018) 3001–3013.
[15] Anatoliy Kovalchuk, NataliiaLotoshynska, Michal Greguš, Ivan Izonin, Leonid Berezko. The 6th International Symposium on Emerging Inter-networks, Communication and Mobility (EICM) August 19-21, 2019, Halifax, Canada.Procedia Computer Science 155 (2019) 630–635.
[16] ȘtefanNiculaa*, Răzvan Daniel Zotaa.The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019) November 4-7, 2019, Coimbra, Portugal , Procedia Computer Science 160 (2019) 9–14.
[17] DevendrasinhVashia, H B Bhadkab, Kuntal Patelc, Sanjay Gargd : International Conference on Computational Intelligence and Data Science (ICCIDS 2019). Procedia Computer Science 167 (2020) 2437–2444.
[18]ZeinabEl-Rewinia, KarthikeyanSadatsharana, Daisy Flora Selvaraja, SibyJosePlathottamb, Prakash Ranganathana, Vehicular Communications 23 (2020) 100214.
[19] Jyoti Tripathia, Anu Saini, Kishan, Nikhil, Shazad. International Conference on Computational Intelligence and Data Science (ICCIDS 2019), Procedia Computer Science 167 (2020) 323–333.
[20] Gayatri S Pandi (Jain)a, Saurabh Shahb, K.H.Wandra.. Conference on Computational Intelligence and Data Science (ICCIDS 2019) Procedia Computer Science 167 (2020) 163–173.