

Security Building into I-Button

M. Venu gopal^{1*}, E.G. Rajan²¹Professor in ECE Department Megha Institute of Engineering and echnology for women²President Pentagonam Research Center***Corresponding author:**

M. Venu gopal, Professor in ECE Department Megha Institute of Engineering and echnology for women .

Submitted: 13 Oct 2022; **Accepted:** 20 Oct 2022; **Published:** 29 Oct 2022**Citation:** Gopal, M. V., Rajan, E. G. (2022). Security Building into I-Button. *J Math Techniques Comput Math*, 1(1), 41-47.**Abstract**

Recent developments in VLSI design using nano devices and the relevant state of the art methodologies have made latest smarter systems available for critical use. Such smart devices could be found in the general market for use with systems pertaining to telecommunications, image processing, mechatronics and so on. One of the security authentication methods used for smart device applications is I-button technology. I-button consists of a memory chip which is enclosed in a stainless steel can of 16 mm thickness. This can is attached to a key fob and a ring. I-button could be used not only for access control applications like computer usage and building entry but also be used as a support device for asset management and data-logging. Every I-button has a unique device address embedded in chip itself meaning all I- buttons come with their already designated addresses. Since I- buttons are fabricated with their stored unique chip addresses, and also user information is stored in EEPROM for user authentication, one can enhance communication security to second level [1].

Introduction

The objective of this paper is to generate a robust technique for unique I-button based customer authentication in a secured client-server transaction. In order to substantiate the worthiness of the techniques and methodologies advocated in this paper as a feasible solution to enhance security level in I- button based transaction, it is required to explore already available techniques researched and used for the same purpose. Bernhard Linke, the principal member (Technical Staff) from 'Maxim Integrated' a company in Dallas, explains in his tutorial titled 'Overview of 1-wire technology and its communication (1706)' technical details of 1-wire devices and their applications [2]. 'Maxim integrated' a company in Dallas, explains in its white paper 8, a tutorial titled 'Data security focusing on encryption (1201)' is on white paper 8, discusses on, an arguably more valuable aspect is authentication [3]. 'Maxim integrated' further explains in its application note titled 'challenge and response with 1-Wire® SHA Devices (190)' and I-button based authentication for access control [4]. Bernhard Linke, the principal member (Technical Staff) from 'Maxim Integrated' in his application note titled 'How to secure access control through challenge and response authentication (4784)' compares various types of key technology [5]. Another white paper titled 'SHA devices used in small cash systems ' of 'Maxim integrated' explains the I-button based paying modalities for products purchased for a departmental store [6]. Further, its application note titled 'Small Message Encryption using SHA Devices (150)' discusses how Maxim's DS1963S SHA I-button can be used with small micro controllers [7].

The application note titled 'SHA I-button (152)', describes the method by which compares with a threshold value [8]. Tatsuro Sugiyura, have authentication token is verified. Necmettin Caner Göv, discussed in his paper titled 'How to generated true random numbers using stationary Gaussian noise' by sampling and discussed in his paper titled 'Demonstration of 30 G bit/s generation of super-conductive true random number generator' by extracting entropy from an electronic circuit like thermal noise and electronic noises [9, 10]. Tommaso Addabbo, presented in his paper titled 'Pseudo-Chaotic lossy compressors for true random number generation', how a Compression technique is used to generate true random bit [11]. H. Pangratz et al., presented a paper titled 'Pseudo-random number generator based on binary and quinary maximal- length sequences' a method to generate random numbers using decimal numbers [12]. Tony Warnock, in his paper titled 'Random number generators' [13]. Delineated random number sequence in contrast to random number which can be used in various applications. Stojanovski, has discussed in his paper titled 'Chaos-based random number generators' how to realize random numbers practically [14]. Yasutada Oohama, analyzed in his paper titled 'Performance analysis of the interval algorithm for random number generation based on number systems' a unique algorithm for random number generation avid B [15]. Thomas et al., explained in his paper titled 'Gaussian random number generators' [16].

Various algorithms to generate GRNG's, and compared their re-

unit, reads the device ID and user information from the I-button and authenticates after validation. In other words, access is provided to an individual holding the I-button once the user information is found to be correct. Now, the difficulty that an organization may face is that an I-button issued to an employee may be misused by an incognito and thus there could be breach of security. Hence, to avoid breach of security, next level security could be provided by adding another 64 bytes ASCII characters string randomly generated and concatenated with the user 64 bytes ASCII character strings data to form 128 bytes ASCII data.

To increase the security further, a visual cryptography could be applied on these 128 bytes of ASCII data and this is what exactly this thesis talks about.

Many visual cryptography algorithms are available for the black and white and color images [24, 25, 27-29].

The following section discusses proposed visual cryptography method in this thesis.

Basic Details of the Proposed Visual Cryptography

Visual cryptography provides two signatures. Signature 1 is stored at the server data base along with the 64-bit device number and the signature 2 is stored in the I-button. During the authentication process, the user makes a physical contact with the 1-wire receptor on the server side. The server identifies the device number stored in the I-button as well as in the data base and examines signature 1 and signature 2 from the I-button and decrypt the original 128 bytes ASCII data. The decrypted user data is compared with the original user data which is available in the server for a match and then the user given access provided match is found. Before giving access to the user the server generates another signature pattern for the 128 bytes of ASCII data and stores signature 1 in the data-base and signature 2 in the EEPROM of I-button. In so doing, one can expect to have additional security measures in the transaction process.

The use of an I-button for secured transaction using visual cryptography is given in figure 1.2 in the form of a block diagram. A sample string of ASCII characters of length 128 is shown in figure 2.3.

character A is represented in pixel matrix which is of size 7x9 as shown in Fig.2.6.

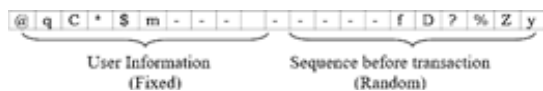


Figure 2.3: Sample string of ASCII characters of length 128 in text form

Assume that this string is to be encoded and loaded in the EEPROM of I-button and the server database after a transaction. It is to be noted that the 64 bytes of user information is always fixed

but the remaining 64 bytes of ASCII data is randomly generated. The server applies a novel visual cryptographic algorithm not on the text data string but on the sequential array of images of the ASCII characters, each character depicted in a lattice of say 7x9 pixels. The sequential image array corresponding to the sequence of ASCII characters in text form as given in figure 2.3 is shown in figure 2.4.



Figure 2.4: Array of graphic images of ASCII characters shown in Fig.1.3

After a secured transaction, the server generates a linear array of 128 visual image patterns each of size 14x18 called signature 1 and its graphical complement called signature 2. Then the server loads signature 2 in the EEPROM of the I- button and retains signature 1 in the database for further transaction. Thus, security is protected every time a transaction is made.

Fig. 2.5 shows a flow diagram as to how the entire transaction process is carried out.

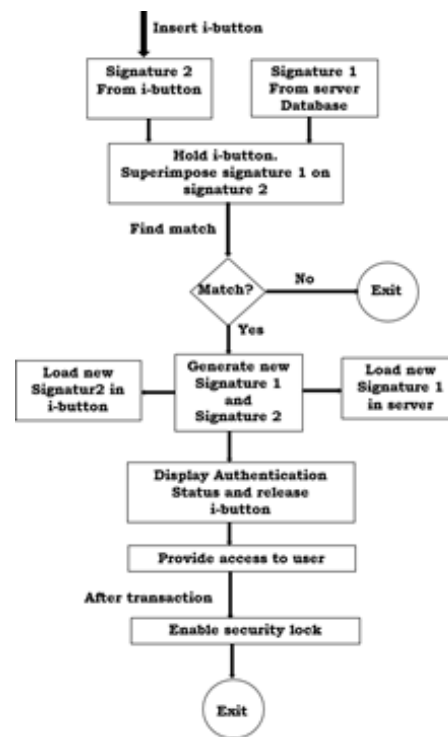


Figure 2.5: Flow diagram of the entire transaction process the very first operation that the server has to do is that each and every ASCII character is represented in a pixel array of size 7x9. This array size is given here just to exemplify the intended operation and one can choose any array size for representing an ASCII character. For example, the ASCII

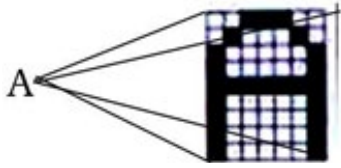


Figure 2.6: ASCII A is represented as pixels in matrix form Fig. 2.7 shows the array representation of 128 ASCII characters.

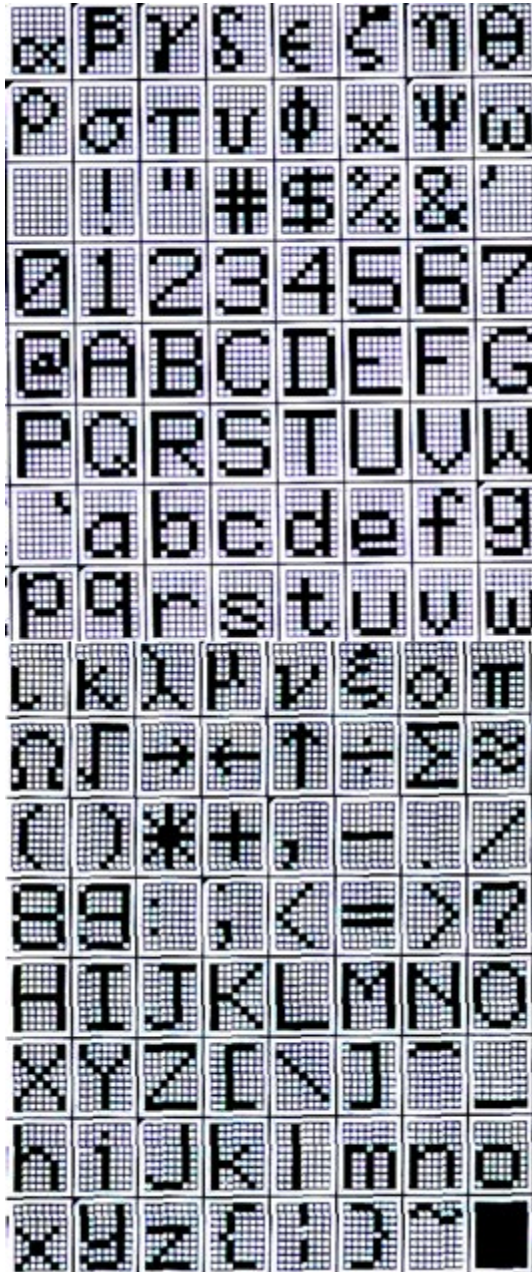


Figure 2.7: Array representation of certain ASCII characters the notion of ‘signatures 1 and 2’ is briefly explained here.

Let us consider the ASCII character ‘f’. The 7x9 array representation of the ASCII character ‘f’ is shown in Fig. 2.8.

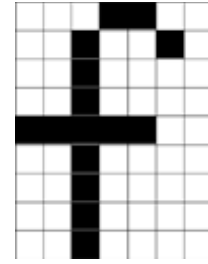


Figure 2.8: Array representation of character ‘f’






The server applies a novel visual cryptographic algorithm on the 7x9 binary valued image (solid white and solid black) array using a code map given in Table 1.1. As per this code map, a binary valued cell, be it solid white or solid black, is either mapped on to a 2x2 cell pattern, visually represented as  and labeled as R, or as a pattern, visually represented as  and labeled as Я. Superimposition of R onto itself yields R. Similarly superimposition of Я onto itself yields Я. Now, both of the resulting patterns R and Я are interpreted here as a half white pattern, visually represented as . In other words, superimposition of identical patterns yields intensity modulation, that is, the resulting pattern would appear to be half white in intensity. Alternatively, superimposition of R onto Я yields a solid black pattern, visually represented as . This means that the input binary image of size 7x9 consisting of solid white and solid black cells would be encrypted [57] [62] as one binary image of size 14x18 consisting of solid white and solid black cells called ‘signature 1’ and another binary image of size 14x18 consisting of solid white and solid black cells called ‘signature 2’. Superimposition of ‘signature 1’ and ‘signature 2’ would yield a binary image of size 14x18 consisting of half white and solid black cells. For example, let us take the case of the image array  corresponding to the ASCII character ‘f’.

Fig.2.9 shows binary image of size 7x9 projected as the binary image of size 14x18. It is to be noted that the 7x9 array has solid white cells and solid black cells whereas the 14x18 array has half white cells and solid black cells after the encryption decryption process.

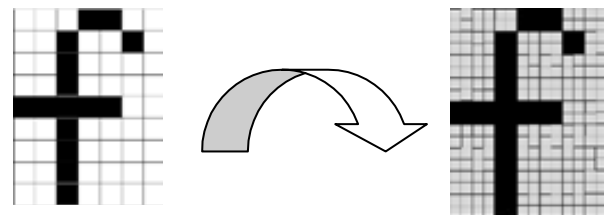


Figure 2.9: Images before and after visual encryption and decryption.

The visual encryption code is given in Table 1.1 Table 1.1: Code map using a 2x2 cell array

| Input Cells (1x1) | Cell Color Before coding | Pattern for signature 1 | Pattern for signature 2 | Both signatures Superimposed | Cell Color after decoding | Projected Cells (2x2) |
|-------------------|--------------------------|-------------------------|-------------------------|------------------------------|---------------------------|-----------------------|
| Solid White | □ | ■ □ | ■ □ | ■ □ | ■ □ | Light Gray |
| Solid White | □ | ■ □ | ■ □ | ■ □ | ■ □ | Light Gray |
| Solid Black | ■ | ■ □ | ■ □ | ■ □ | ■ □ | Solid Black |
| Solid Black | ■ | ■ □ | ■ □ | ■ □ | ■ □ | Solid Black |

Table 1.2: Code map using a 3x3 cell array

| Input Cells (1x1) | Cell Color Before coding | Pattern for signature 1 | Pattern for signature 2 | Both signatures Superimposed | Cell Color after decoding | Projected Cells (2x2) |
|-------------------|--------------------------|-------------------------|-------------------------|------------------------------|---------------------------|-----------------------|
| Solid White | □ □ □ | ■ □ □ | ■ □ □ | ■ □ □ | ■ □ □ | Dark Gray |
| Solid White | □ □ □ | ■ □ □ | ■ □ □ | ■ □ □ | ■ □ □ | Dark Gray |
| Solid Black | ■ ■ ■ | ■ □ □ | ■ □ □ | ■ □ □ | ■ □ □ | Solid Black |
| Solid Black | ■ ■ ■ | ■ □ □ | ■ □ □ | ■ □ □ | ■ □ □ | Solid Black |

The visual encryption of an image yields two different arrays of patterns called ‘signature 1’ and ‘signature 2’, which are graphical complements the superimposition of which yields the projected image. For example, one type of ‘signature 1’ and its graphical complement are shown in figure 1.10 (a) and (b) respectively. From Fig.2.10, it is clear that the image to be encrypted is basically a binary image consisting of two shades, viz solid black and solid white, whereas the decrypted image is a binary image consisting of two shades, viz solid black and gray. During the interpretation process, one can consider the gray cells as solid white cells.

Complexity Analysis

A pixel array matrix corresponding to an ASCII character consists of two values, that is, a ‘0’ and a ‘1’. Let the number of 1’s in the binary pattern of an ASCII character be ‘n’ and that of 0’s be ‘k’, so that the total number of cell values in the pixel array is n+k. Consider a 2x2 neighborhood structure. In this case, any of the eight signature pairs could be used to encode each ‘1’. Assume that there are ‘n’ number of ‘1’ and ‘k’ number of ‘0’. Then one can have 16n random possibilities of encrypting all 1’s and 16k random possibilities of encrypting all 0’s. Table 1.3 shows the encryption map for 1’s and 0’s when 2x2 matrix is used for neighborhood generation.

Table 1.3: Encryption map for 2x2 neighborhood

| Encryption pair for ‘1’ | | Encryption pair for ‘0’ | |
|-------------------------|--------------|-------------------------|--------------|
| Signature #1 | Signature #2 | Signature #1 | Signature #2 |
| 0000 | 0000 | 0000 | 1111 |
| 0001 | 0001 | 0001 | 1110 |
| 0010 | 0010 | 0010 | 1101 |
| 0011 | 0011 | 0011 | 1100 |
| 0100 | 0100 | 0100 | 1011 |
| 0101 | 0101 | 0101 | 1010 |
| 0110 | 0110 | 0110 | 1001 |
| 0111 | 0111 | 0111 | 1000 |
| 1000 | 1000 | 1000 | 0111 |
| 1001 | 1001 | 1001 | 0110 |
| 1010 | 1010 | 1010 | 0101 |
| 1011 | 1011 | 1011 | 0100 |
| 1100 | 1100 | 1100 | 0011 |
| 1101 | 1101 | 1101 | 0010 |
| 1110 | 1110 | 1110 | 0001 |
| 1111 | 1111 | 1111 | 0000 |

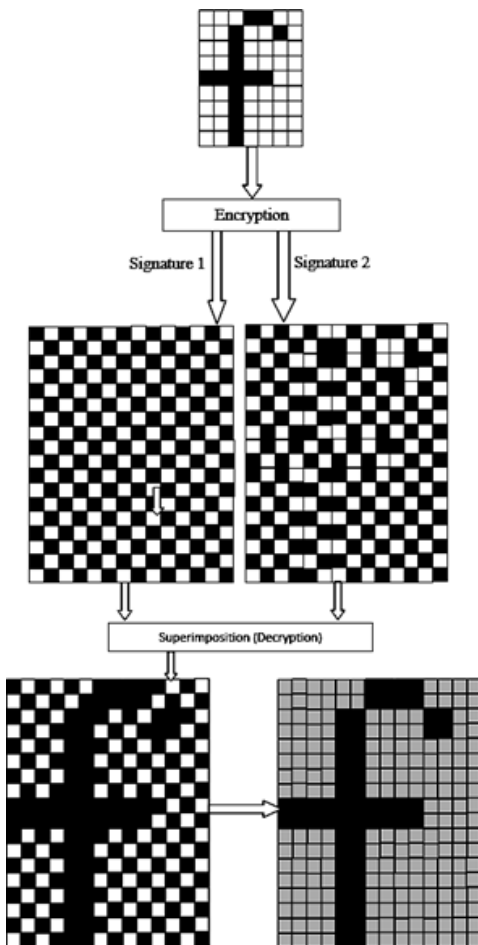


Figure 2.10: Signatures 1 and 2, their superimposition and projection

Alternatively, one can use a code map using a 3x3 cell array as shown in table 1.2 for the purpose of visual encryption

It is to be noted that one can use any of the 16 visual patterns to encrypt 1's and 0's. The pairs shown in shaded region of table 1.3 are the inverted pairs shown above the shaded region.

Enhance the security features in I-button based access control and communication.

Presently I-button technology is used in various access control, security and authentication applications supported by secured hash authentication and multiple password protection schemes. These kinds of security techniques are not robust and they are found to be amenable for hacking with minimum efforts.

To enhance the security level in this context, random number generation using thermal noise is considered and a prototype hardware designed and developed. It was observed that the random numbers generated using this hardware facility yielded sequences with large entropy. To enhance the security to next level, visual cryptography using cellular automata has been introduced. Further complexity analysis has been verified and found that, it is impossible for a hacker to decode the information in signatures in short time. As future work, the results found in this thesis could be applied to other security authentication devices like ATM, RFID, Smart card etc., without changing their corresponding security protocols.

Compliance with Ethical Standard

I thank Dr.E.G.Rajan for the research support given to me while preparing this manuscript. The manuscript is prepared with proper understanding and assessment of the content. The financial support to research and publish paper is not a conflict between the authors, as financial matters are supported by author Dr.M.Venu gopal. The author supports money through his monthly salary. We declare that we have not received any financial support from any organization. Publish of manuscript in the journal is purely academic interest. We declare that we do not have any conflict of interest in publishing this paper.

We state that no involvement of animals in our research and this article studies does not involve human participation in the research. Also, this research and manuscript has not handled any confidential data.

Competing Interest

There is no financial and non-financial interest to undermine the objectivity, integrity and values of publication by the influence of the authors related to data analysis and interpretation. Also, the financial competing interests, potential employment interest, personal financial interest, non-financial interest does not exist in publishing this manuscript.

Research Data Policy and Data Availability Statement

We state that all the data in this manuscript is original and authors have no reservations in sharing the data available in the manuscript.

So, one can expect $16(n+k)$ coding patterns in visual cryptography when 2×2 matrix is used for neighborhood generation.

Conclusions

This thesis provides results due to a comprehensive study made on the problem of identifying a feasible solution to

References

1. Wang, R. Z., & Hsu, S. F. (2011). Tagged visual cryptography. *IEEE Signal Processing Letters*, 18(11), 627-630.
2. Linke, B. (2008). Overview of 1-Wire Technology and Its Use. MAXIM, AN1796, jun.
3. Maxim integrated, " 1-Wire® SHA-1 Overview ", TUTORIAL 1201 White Paper 8, 2002
4. Maxim integrated, " Challenge and Response with 1- Wire® SHA Devices", application note 190 (3), 2002
5. Bernhard Linke, "Secure Access Control Through Challenge and Response Authentication", Maxim integrated, Principal member technical staff, application note 4784, 2011
6. Maxim integrated, "SHA Devices Used in Small Cash Systems", White Paper 1.
7. Maxim integrated, "Small Message Encryption using SHA Devices", application note 150, 2002.
8. Maxim integrated, "SHA iButton Secrets and Challenges", application note 152, 2002
9. Göv, N. C., Mihçak, M. K., & Ergün, S. (2010). True random number generation via sampling from flat band-limited Gaussian processes. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 58(5), 1044-1051.
10. Sugiura, T., Yamanashi, Y., & Yoshikawa, N. (2010). Demonstration of 30 Gbit/s generation of superconductive true random number generator. *IEEE transactions on applied superconductivity*, 21(3), 843-846.
11. Addabbo, T., Fort, A., Kocarev, L., Rocchi, S., & Vignoli, V. (2011). Pseudo-chaotic lossy compressors for true random number generation. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 58(8), 1897-1909.
12. Pangratz, H., & Weinrichter, H. (1979). Pseudo-random number generator based on binary and quinary maximal-length sequences. *IEEE Transactions on Computers*, 28(09), 637-642.
13. Tony warnock, "Random number generators", Los Alamos Science Special Issue 1987, 137 - 141
14. Stojanovski, T., Pihl, J., & Kocarev, L. (2001). Chaos-based random number generators. Part II: practical realization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 48(3), 382-385.
15. Oohama, Y. (2011). Performance analysis of the interval algorithm for random number generation based on number systems. *IEEE transactions on information theory*, 57(3), 1177-1185.
16. Thomas, D. B., Luk, W., Leong, P. H., & Villasenor, J. D. (2007). Gaussian random number generators. *ACM Computing Surveys (CSUR)*, 39(4), 11-es.

17. Seredynski, F., Bouvry, P., & Zomaya, A. Y. (2004). Cellular automata computations and secret key cryptography. *parallel computing*, 30(5-6), 753-766.
18. Cheung, R. C., Lee, D. U., Luk, W., & Villasenor, J. D. (2007). Hardware generation of arbitrary random number distributions from uniform distributions via the inversion method. *IEEE transactions on very large-scale integration (VLSI) systems*, 15(8), 952-962.
19. Marsaglia, G., & Tsang, W. W. (2002). Some difficult-to-pass tests of randomness. *Journal of Statistical Software*, 7, 1-9.
20. Gutterman, Z., Pinkas, B., & Reinman, T. (2006, May). Analysis of the linux random number generator. In *2006 IEEE Symposium on Security and Privacy (S&P'06)* (pp. 15-pp). IEEE.
21. Naor, M., & Shamir, A. (1996, April). Visual cryptography II: Improving the contrast via the cover base. In *International Workshop on Security Protocols* (pp. 197-202). Springer, Berlin, Heidelberg.
22. Zhou, Z., Arce, G. R., & Di Crescenzo, G. (2006). Halftone visual cryptography. *IEEE transactions on image processing*, 15(8), 2441-2453.
23. Ross, A., & Othman, A. (2010). Visual cryptography for biometric privacy. *IEEE transactions on information forensics and security*, 6(1), 70-81.
24. Zhang, C. N., Yu, Q., & Liu, X. W. (2010, November). Multiple Dimensional Fault Tolerant Schemes for Crypto Stream Ciphers. In *2010 International Conference on Multimedia Information Networking and Security* (pp. 406-412). IEEE.
25. Kang, I., Arce, G. R., & Lee, H. K. (2010). Color extended visual cryptography using error diffusion. *IEEE Transactions on Image Processing*, 20(1), 132-145.
26. Gupta, P. K., Hemrajani, N., Shiwani, S., & Davey, R. (2012). Halftone based Secret Sharing Visual Cryptographic Scheme for Color Image using Bit Analysis.
27. Loganathan, D. (2011, July). Color image cryptography scheme based on visual cryptography. In *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies* (pp. 404-407). IEEE
28. Wu, X., & Yang, C. N. (2020). Probabilistic color visual cryptography schemes for black and white secret images. *Journal of Visual Communication and Image Representation*, 70, 102793.
29. Prema, G., & Natarajan, S. (2013, February). Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application. In *2013 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 727-730). IEEE.

Copyright: ©2022 M. Venu gopal. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.