Research of High Speed and Energy Efficient Visual Cryptography Techniques

V.Arun, Rajashekhar C Biradar, V.Mahendra

Abstract— Visual cryptography is the most popular technique attracted various researchers to improve the security level while utilizing the images and videos as encryption key, instead of text which is easy to crack. Visual cryptography processes the multimedia information such as images, videos and audios in order to enhance the security of the multimedia data. Visual cryptography computes complex multimedia information which may leads to computational overhead when simple processing techniques and architectures were utilized. So, various researchers had taken over this challenge and trying to resolve while introducing the various high speed techniques and architectures which would make visual cryptography process highly secured and energy efficient. This article presents a literature review on various high speed architectures and visual cryptographic techniques which have been adopted for processing multimedia data. This review provides the survey of different visual cryptography techniques adopted to achieve better security and also discusses their advantages and limitations. The comparison has been made on different visual cryptography methods with respect to performance, level of security and PSNR.

Keywords:Visual cryptography, security, energy efficient, high speed architecture, accurate prediction outcome

I. INTRODUCTION

Visual cryptography is the process of encrypting the multimedia contents such as images, videos and audios etc. [1], Visual cryptography appears to be more complex task where the visual data needs to be encrypted without losing the original visual content information [2]. In recent world, various research applications such as data security [3], data hiding would requires to handle visual information for the improved performance [4].Most of the organization started to concentrate on data security and hiding techniques due to increased usage of computer generation. To achieve this organizations spend millions of amount, thus the security of their industries can be ensures. This is done due to increased threaten towards cyber theft and crime. Increased technologies made easier environment for the criminals to involve in the cyber crime activities with partial known information about the industrialists [5]. These issues can be resolved by introducing the cryptography techniques. Particularly visual cryptography plays major part in the increased security level due to its complexity level. Encryption process involved in the visual cryptography technique increased its applicability and usage in various areas[6]. In this research work, discussion about those particular areas has been given. The specific applications that utilizes the visual cryptography techniques are Biometric security [7], Watermarking [8], Remote electronic voting [9], Bank customer identification [10] etc.

Another issue that found mostly is the transmission of multimedia data through unknown network which is found to be more threatened issue in the 21st century [11]. Secured and reliable transmission of multimedia data through the network required to introduce the various security techniques which needs to be applied before sharing the personal information through the public network. In this analysis work, discussion about the various research techniques that aims to improve the security level while transmitting the multimedia data through unsecured medium has been discussed. The different ways that are available to enhance the security level while transmitting the data. Those possible ways are password, image hiding, watermarking, authentication and identification [12].However this technique might be failed to ensure the security while transmitting the data through single transmission medium. This data will be lost or corrupted when the single transmission medium is failed. In today world visual cryptography is found to be most common solution for protecting the visual content [13]. In this research, discussion about the techniques that involved in the secret image sharing through public network is discussed in detailed with the recent techniques such as communication technology and information security.

The research is to design and present an energy efficient architecture for visual cryptography. In this research work, study about the various visual cryptography techniques has been given along with their working procedure and the processing flow. This analysis work also provides the discussion about the different high speed and energy efficient architecture. From this research study authors can gain the overall view about the working procedure and the processing flow of different research methods. And also authors can study the merits and demerits of various research methodologies which can lead to improved performance.

The overall view of analysis work is given as follows: In this section overall introduction about the role of visual cryptography and the need of the high speed architecture has been given. In this section 2, discussion about the different related research methodologies which attempts to performance visual cryptography is provided with their working procedure. In section 3, discussion about the

Revised Manuscript Received on September 10, 2019.

V.Arun, Research Scholar, School of Electronics and Communication Engineering, Reva University, Bengaluru, Karnataka, India

Rajashekhar C Biradar, Professor and Director, School of Electronics and Communication Engineering, REVA University, Bengaluru, Karnataka, India.

V.Mahendra, Professor, Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, Telangana, India

different high speed and energy efficient architecture has been given. In section 4, comparison evaluation of the different research techniques in terms of merits and demerits is given. Finally in section 5 conclusion of the analysis work is given.

II. OVERVIEW OF VISUAL CRYPTOGRAPHYTECHNIQUES

In this section,we discuss various visual cryptography techniques that are introduced by different researchers.

Lee and Chiu [14] introduced the Extended Visual Cryptography Scheme (EVCS) for ensuring the security level for the general access structure. This research method would integrate the cover images for each share. This process is done in two steps to improve the security level of general access structure. In the first step meaningless cover images will be generated for each individual image share. This generated cover images will be integrated with the each image share in the second step by applying the stamping algorithm. This method ensures the improved security level of General Access Structure. Wang et al [15] introduced the contrast visual cryptographic technique namely Traditional VCS schemes without reversing (nRVCS) with the applicability of reversing technique in order to ensure the security level of secret image sharing process. This research method ensures the guaranteed reconstruction of quality while performing the visual cryptography technique. The main goal of this research method is to improve the contrast level of the shared multimedia data with guaranteed image quality. This method guarantees the optimal contrast enhancement even with the presence of minimal amount of shares. Shyu [16] introduced theRevised Visual cryptosystem for general access structure (RVC-GAS). This method attempts to implement the novel visual cryptosystem for ensuring the security level of the general access structure. This is done by revising the security issues of general access system. In this research work, image shares will be altered by modifying the secret shares of n participants which will increase the security level of general access structure. This method do not require any pixel expansion to guarantee the security level. The performance evaluation of the research method guarantees the increased flexibility and reliability of the security level of visual cryptosystem. Li et al [17]introduced the binary region incrementing visual cryptography scheme (BRI-VCS) to ensure the security level. This method attempts to secure the system even with the presence of multiple image shares with different contrast level. The quality of the reconstructed image is ensured by introducing the integer linear programming based binary (k,n) method. This method would maintain the secrecy of image shares with same and different contrast level. This method ensures the better performance level even with the presence of larger pixel expansion.

Sethi and Kapoor [18] introduced the novel architecture for the steganography process to ensure the effective data hiding outcome. This is done in this work by introducing the Genetic algorithm based steganography and cryptography (GASC) which ensures the improved security level. This method ensures the increased security level by transforming the digital media into unreadable format. This is done by introducing the AES cryptographic algorithm by using which encryption of data contents is done. And then genetic algorithm is applied for the pixel arrangement of images thus the data hiding is performed effectively. Shankar and Eswaran [19] performed the secured image sharing by introducing the Elliptic curve cryptography (ECC)technique. This method would improve the security level by performing the multiple share creation method in which the image will divided into multiple shares based RGB values which will then be encrypted in order to ensure the security level. Here the multiple share of image is generated by adapting the new fangled technique which will then be encrypted and decrypted utilizing the elliptic curve cryptographic technique.

Usman et al [20] introduced the lightweight, robust and efficient scheme (LWRES) for the encryption purpose to perform the data exchange between the cloud and mobile devices. This is done by performing the data hiding process which would encode the High efficiency video coding on the video streams. And also this method ensures the security level by introducing the advanced encryption standard by using which encryption of image shared will be done. The evaluation of this method ensures the better performance with reduced processing time and the increased data size. Hamza [21]performed image cryptography by introducing the novel algorithm which is based on pseudo random number sequence generator (PRSGA). This method would create the cryptographic keys for the different digital images by using cryptographic applications. This is done by introducing the non uniform probability distribution procedure based on which multiple cryptographic keys are generated. This method ensures the increased security level with guaranteed robustness, better speed and improved effectiveness. This method can protect against the multiple differential attacks by successfully introducing the security scheme.

Yan et al [22] introduce the analysis by synthesis (abS) method to perform the encoding process. In this method, reconstruction of the images is done by utilizing the multiple shares of the images that are collected from the encoder process and then error between the reconstructed secret and the original secret images are differentiated. This is done by introducing the error diffusion process which would find the exact difference between the original image and reconstructed image more accurately. This framework is known to be more simpler and flexible with varying pixel intensities. The taxonomy of the above discussed research methods has been given in Figure 1

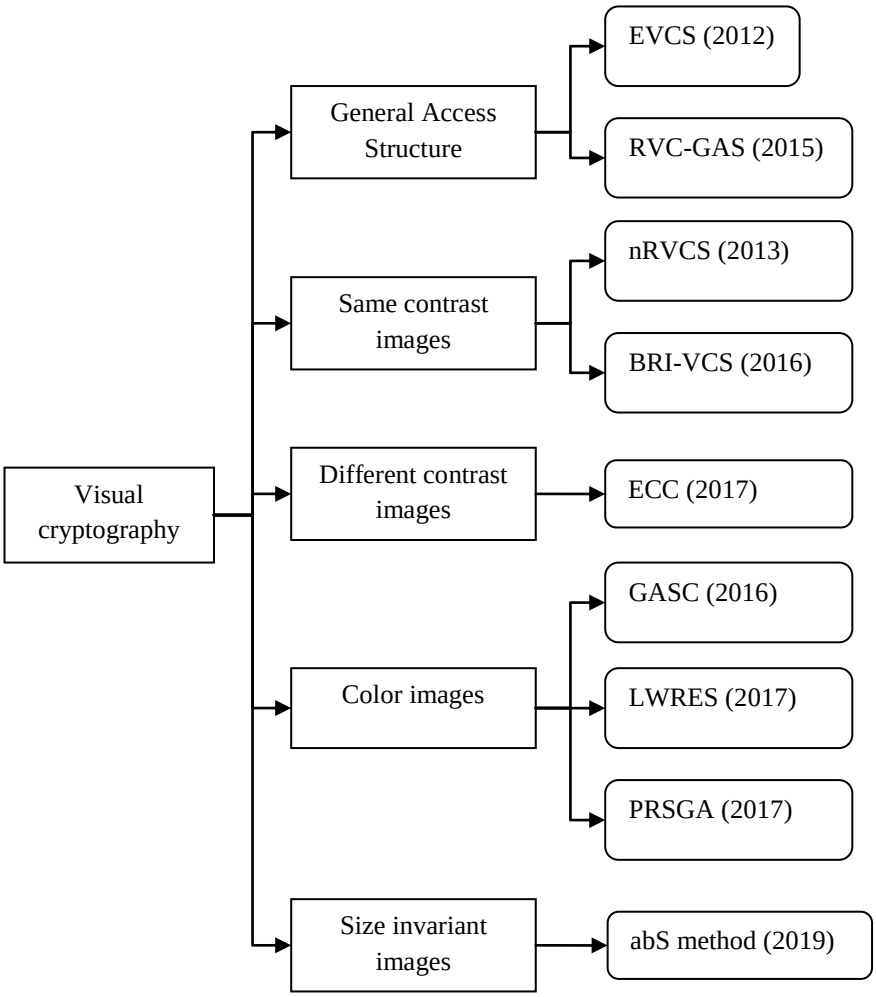

Figure 1. Taxonomy of visual cryptography techniques

In figure 1, taxonomy of the visual cryptography techniques has been given. Each research technique adapts the different procedures for ensuring the quality and security level of images. Here some of the research techniques are applied on the gray scale images whereas some techniques applied for the color images. All these methods attempts to perform visual cryptography without compromising the contrast of images. From this taxonomy it is proved that the abS method can ensure the increased security level with enhanced contrast level. And also this method can handle size invariant images whereas other methods can perform cryptography on similar size images alone. And also abS method can handle images with different contrast level whereas method can perform well on images with same contrast except ECC method.

III. HIGH SPEED AND ENERGY EFFICIENT CRYPTOGRAPHIC ARCHITECTURES

In this section discussion about the various research methodologies which attempts to provide the high speed and energy efficient architecture for performing the complex cryptographic operations are discussed. Kuang et al [23] attempted to speed up the RSA cryptosystem process by integrating the carry adder package with the high speed architecture. This is done by introducing the montgomery modular multiplication algorithms which perform calculations in the parallel way. The main goal of this research work is to provide the environment for the cryptographic operations which can perform calculation fastly and in the energy efficient way. And also this proposed architecture confirms the increased throughput level thus much encryption process can be carried out within short period. Vollala and Ramasubramanian [24] attempted to improve the performance of cryptographic operations by optimizing the modular exponentiation and modular multiplication process. This method guarantees the increased efficiency of modular exponentiation process by reducing the frequency of modular multiplication. Thus the energy efficiency can be achieved along with the improvised throughput. The evaluation of this research method is carried out on two different methods namely Bit Forwarding 1 bit (BFW1) and the Bit Forwarding 2-bits (BFW2) which is extended version of tradition exponential algorithm.

Vollala et al [25] proposed upgrades to the Montgomery Multiplication and furthermore to Square and Multiply calculation. Bit Forwarding 1-bit (BFW1) calculation has been executed to assess measured exponentiation that brought about 11.11% enhancement in throughput, and 1.90% decrease in power utilization. A Dual-center RSA processor with an equipment scheduler has been intended for performing simultaneous cryptographic changes to achieve better throughput without expanding the recurrence.Huo and Liu [26] proposed a programmable

ASIP structure for four kinds of the bit-wise calculations: square figures, stream figures, Reed-Solomon (RS) Codes, and Cyclic Redundancy Check (CRC). We accomplish this through discovering the calculation likenesses and the ideal parallel degree (128-piece) among the four kinds of bit-wise calculations. The adaptability of our plan can develop the scope of uses and broaden the time-in-market of a SoC. Moreover, our structure accomplishes ASIC-like execution, for example, 25.6 Gb/s for AES encryption, 17.6 Gb/s for RS(255,239) interpreting, and 281.6 Gb/s for CRC figuring, and so forth with 0.19 mm2 (28 nm) silicon region.Li et al. [27] have suggested that the utilization of reconfigurable equipment for location of interruptions would improve the system security framework. The execution hole between the execution speed of security programming and the sheer measure of information to be prepared is augmenting, and this is a difficult issue. Therefore, to address this, it is basic to begin executing equipment arrangements in situations requiring high security.

Progressed cryptographic methods, for example, hash capacities and message verification codes, are presently being utilized in current frameworks managing capacity and control of touchy information. An investigation by Nickolas and Sivasankar [28] has stated that such calculations are unreasonably requesting to be executed in programming for the handling speeds anticipated today in an installed framework. Along these lines, equipment parts must be utilized to understand the equivalent in a productive way. An article by Villasenor et al. [29] states that present FPGAs can be reconfigured inside a millisecond, and at last, they will most likely adjust persistently – which means, they can be reinvented each 10-3 s (or less).This makes them profoundly appropriate for structure encryption frameworks, and executing calculations, for example, the DES, AES, and hash capacities with higher speed and effectiveness. An audit paper by Tonde and Dhande [30] clearly entireties up the writing reviewed. A case of a high-security application, electronic exchanges, has been taken. A FPGAbased execution of the AES is unmistakably appeared as having various favorable circumstances, including simplicity of calculation alteration dependent on the application, engineering productivity, higher throughput, low idleness and cost effectiveness.

The taxonomy of the above discussed research methods have been given in Figure 2.

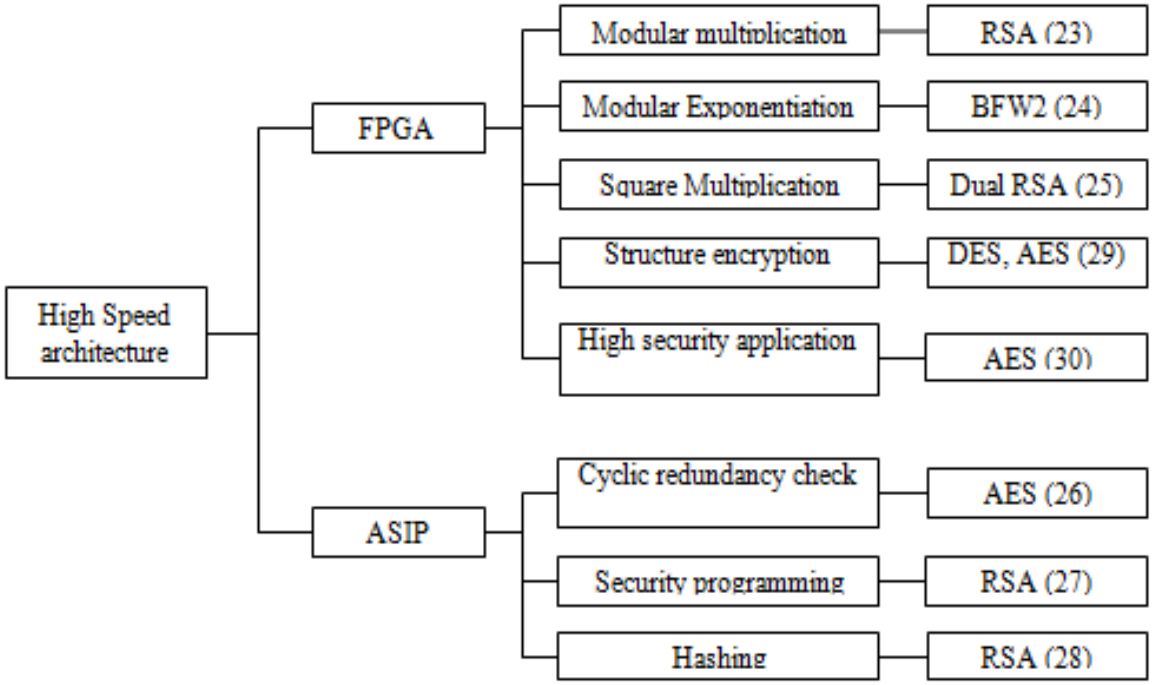

Figure 2. Taxonomy of High speed architecture

In figure 2, taxonomy of the high speed architecture has been given. Each research technique adapts the different procedures for ensuring the quality and security level of images with increased computation speed.

IV. COMPARISON ANALYSIS OF VISUAL CRYPTOGRAPHIC TECHNIQUES

In this section, comparison evaluation of the different visual cryptography research techniques is given in terms of merits and demerits of each method. In the following comparison table 1, comparison of the each research techniques in terms of merits and demerits is given.

Table 1. Comparison of different visual cryptography techniques

S.No	Authors	Method	Merits	Demerits
1	Lee and Chiu [2012]	EVCS	Supports the adjustable density of cover images Increased security level with ensured modularity	Increased complexity while constructing the General Access Structure
2	Wang et al [2013]	nRVCS	Guaranteed satisfaction of multiple user requirements Better reconstruction quality Improved contrast enhancement	Performance degradation with the presence of noisy features
3	Shyu [2015]	RVS-GAS	Improved flexibility Guarantees the flawless pixel expansion with ensure security level	Reduced reconstructed quality with the presence of light contrast Reduced security level with high depth intensity of pixels
4	Li et al [2016]	BRI-VCS	Achieves balanced trade-off between the contrast and the security level Ensures more effective and feasible solution	More computational complexity Less flexibility
5	Sethi and Kapoor [2016]	GASC	Optimal steganography outcome Better security enhancement result	It requires more processing cycles to accomplish the task
6	Shankar and Eswaran [2017]	ECC	Reduced mean squared error value Improved correlation coefficient with ensured image quality	Image quality might get affected with the presence of increased noise level
7	Usman et al [2017]	LWRES	Reduced processing time Increased data size	Reconstruction quality is not guaranteed Degraded decoding performance
8	Hamza [2017]	PRSGA	Increased security level This method perform better security level with the presence of large number of pixels	Might degraded in its performance by generating the random number value
9	Yan et al [2019]	abS method	Guaranteed security level Improved flexibility More simpler network	Limited to error diffusion The values of neighbouring pixels would affect the security level
Comparison evaluation of high speed and energy efficient architecture				
1	Kuang et al [2013]	Energy efficient high speed architecture	Reduced energy consumption Increased throughput Improved cryptographic performance	Need to concentrate on energy surfing factor which would increase the energy consumption
2	Vollala and Ramasubramanian [2017]	Energy Efficient modular exponential algorithm	Increased throughput Energy efficient cryptographic operation	It is not realistic enough to support the real time operations
3	Vollala et al [2017]	Enhanced Montgomery Multiplication algorithm	The proposed research method is scalable Improved energy efficiency outcome	More computational overhead
4	Huo and Liu [2018]	Programmable ASIP structure	Guaranteed high speed performance Improved energy efficiency	Increased Running time

V. INFERENCE FROM THE DISCUSSION & RESULTS

In the above section, discussion about the different research methodologies has been given in terms of their working procedure merits and demerits. Each research method focuses on ensuring the better visual cryptography performance in order to secure the data while transmitting through unknown medium.From the analysis from various research methods, it is confirmed that the performance of the visual cryptography depends on the visual quality of the reconstructed images. This is achieved in the existing research methods by following different procedures. Among those methods, Analysis-by-Synthesis (AbS) Approachis found to be better research method than the other techniques.

This method is proposed by Yan et al [22] to perform encryption on the grey scale images. The main goal of this research work is to improve the visual quality of the images with ensured security level. This method improves the visual quality of images without considering the different size invariants whereas in the existing work visual quality is enhanced only for the images with similar size. This AbS

framework is simple and flexible in that it can be combined with many existing size-invariant VC algorithms, including probabilistic VC, random grid VC, and vector/block VC. More importantly, it is proved that this AbS framework is as secure as the traditional VC algorithms.In the following table comparison of different performance metrics has been given.

Table 2. Performance Metric

Methods	Image type	Pixel Expansion	Contrast	Complexity	PSNR	MSE	CC
Extended Visual Cryptography Scheme (EVCS)	Gray scale	Medium	¼ decreased contrast	O(nhw)	-	-	-
Traditional VCS schemes without reversing (nRVCS)	Gray scale	Low	Nearest to upper bound value	O(k)	-	-	-
Revised Visual cryptosystem for general access structure	Color image	No	Less contrast and it is different for images	-	-	-	-
Binary region incrementing visual cryptography scheme	Color image	High	Same contrast	-	-	-	-
Genetic algorithm based steganography and cryptography	Gray scale	-	-	-	-	-	-
Elliptic curve cryptography technique	Color image	-	Less contrast	-	39.0097	9.2797	0.9976
lightweight, robust and efficient scheme	Color image	-	-	-	45.67	-	-
Pseudo random sequence generator algorithm	Color	High	High	n/2	-	-	-
analysis by synthesis method	Gray scale	Low	Less contrast	O(MN)	28	-	-

VI. NUMERICAL COMPARISON

Various performance metrics has been considered to evaluate the improvement of the proposed methodology than the existing methodology in terms of the security level. The performance metrics that are considered in this work are listed as follows:

- Peak signal to noise ratio
- Security level

The comparison is made between the research methodologies namely Traditional VCS schemes without reversing (nRVCS) [2013],

Binary region incrementing visual cryptography scheme (BRIVCS) [2016], Pseudo random sequence generator algorithm (PRSGA) [2017] and analysis by synthesis method (AbS) [2019] and the numerical evaluation are given in the graphical formats

To measure the quality of reconstructed of video or image

PSNR is frequently used. And it is the ratio of the maximum possible power of an input image or video to the power of output image or video.

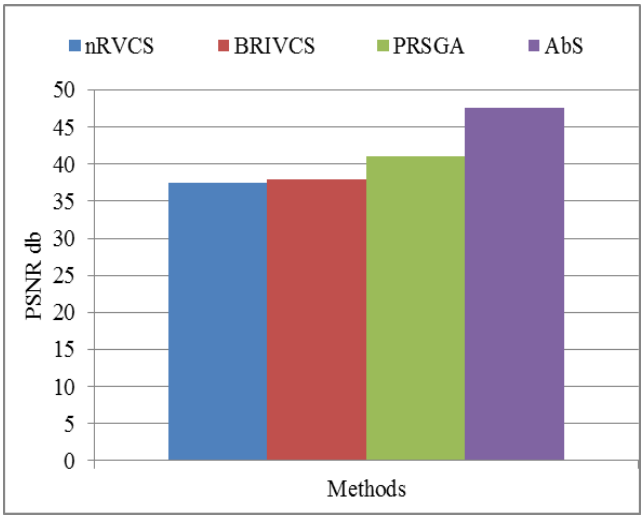

Figure 2. Experimental results against PSNR comparison

The security of a symmetric cryptosystem is a function of the length of the key. The longer the key, the more resistant the algorithm is to a successful brute force attack. For this reason, key length was chosen as the first parameter for specifying cryptographic algorithms. Key Length is an easy objective, numeric metric to adopt since key size is universally expressed as a number of bits.The graphical presentation of the key length is depicted in the figure 3.

In figure 3, Security level is measured in terms of varying key length which is depicted above. From this figure it is confirmed that the security level is increased gradually as the key length is increased. Security level is more for the proposed work than the existing methodology for the different key lengths.

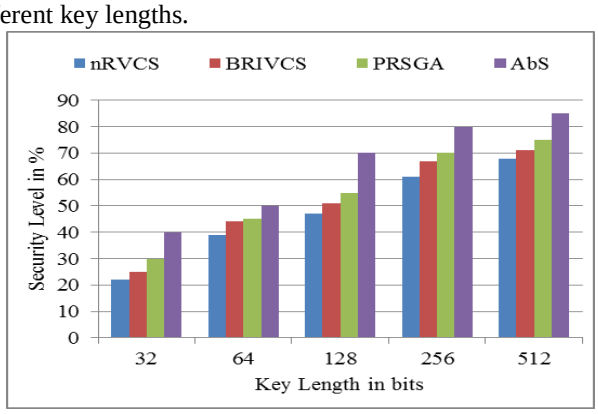

Figure 3. Key Length Vs Security Level comparison

VII. CONCLUSION

In this review, discussion about high speed architecture and the adopted techniques of different visual cryptographic techniques has been presented. This literature review provides the overview of different visual cryptography techniques which tends to achieve better security along with the advantages and limitations of different research techniques. The comparison evaluation of the different research methods has been performed based on performance outcome, security, energy efficiency of the research methods. It is concluded from the analysis, AbS framework found to provide better outcome than the other research methods by supporting the visual quality enhancement without considering image size invariants.

VIII. REFERENCE

1. Cimato, S., & Yang, C. N. (Eds.). (2017). Visual cryptography and secret image sharing. CRC press.
2. Y. Acar et al., "Comparing the Usability of Cryptographic APIs," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 154-171 doi: 10.1109/SP.2017.52
3. Dongpo Zhang “Big data security and privacy protection” in 8th International Conference on Management and Computer Science (ICMCS 2018), Atlantis Press , Advances in Computer Science Research, volume 77
4. Pandey, Anjney and Subhranil Som. “Applications and usage of visual cryptography: A review.” 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (2016): 375-381.
5. Keyser, Mike. "The Council of Europe Convention on Cybercrime." In Computer Crime, pp. 131-170. Routledge, 2017.
6. Yang, Ching-Nung & Liao, Jung-Kuo & Wu, Fu-Heng & Yamaguchi, Yasushi. (2016). Developing Visual Cryptography for Authentication on Smartphones. 189-200. 10.1007/978-3-319-44350-8_19.
7. David Chek Ling Ngo, Andrew Beng Jin Teoh, and Jiankun Hu. 2015. Biometric Security. Cambridge Scholars Publishing, , United Kingdom.
8. A. Cohen, J. Holmgren, R. Nishimaki, V. Vaikuntanathan, D. Wichs, "Watermarking cryptographic capabilities", IACR Cryptology ePrint Archive, vol. 2015, pp. 1096, 2015.
9. Schneider, Alexander & Meter, Christian & Hagemeister, Philipp. (2017). Survey on Remote Electronic Voting.
10. Karpey, D., & Pender, M. (2016). U.S. Patent No. 9,396,730. Washington, DC: U.S. Patent and Trademark Office.
11. Li, H., Li, B., Tran, T. T., & Sicker, D. C. (2016) “Transmission schemes for multicasting hard deadline constrained prioritized data in wireless multimedia streaming” IEEE Transactions on Wireless Communications, 15(3), 1631-1641.
12. Yang, J., He, S., Lin, Y., & Lv, Z. (2017). Multimedia cloud transmission and storage system based on internet of things. Multimedia Tools and Applications, 76(17), 17735-17750.
13. Pawar, P. R., & Borse, M. S. (2016). Transmission Risk Reduction in Image sharing Scheme with Diverse Image Media. International Journal of Advance Research in
14. Science and Engineering, Vol. No. 5, Special Issue No. 01, May 2016.
15. Lee, K. H., & Chiu, P. L. (2012). “An extended visual cryptography algorithm for general access structures” IEEE transactions on information forensics and security, 7(1), 219-229.
16. Wang, D. S,, Song, T., Dong, L., & Yang, C. N. (2013). Optimal contrast grayscale visual cryptography schemes with reversing. IEEE transactions on information forensics and security, 8(12), 2059-2072.
17. Shyu, S. J. (2015). Visual cryptograms of random grids for threshold access structures. Theoretical Computer Science, 565, 30-49.
18. Li, S., Li, J., & Wang, D. (2016). Region incrementing visual cryptography scheme with same contrast. Chinese Journal of Electronics, 25(4), 621-624.

19. Sethi, P., & Kapoor, V. (2016). A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography. Procedia Computer Science, 87, 61-66.
20. Shankar, K., & Eswaran, P. (2017). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14(2), 118-130.
21. Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. Information Sciences, 387, 90-102.
22. Hamza, R. (2017). A novel pseudo random sequence generator for image-cryptographic applications. Journal of Information Security and Applications, 35, 119-127.
23. Yan, B., Xiang, Y., & Hua, G. (2019). Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach. IEEE Transactions on Image Processing, 28(2), 896-911.
24. Kuang, S. R., Wang, J. P., Chang, K. C., & Hsu, H. W. (2013). Energy-efficient high-throughput Montgomery modular multipliers for RSA cryptosystems. IEEE Transactions on very large scale integration (VLSI) systems, 21(11), 1999-2009.
25. Vollala, S., & Ramasubramanian, N. (2017). Energy efficient modular exponentiation for public-key cryptography based on bit forwarding techniques. Information Processing Letters, 119, 25-38.
26. Vollala, S., Varadhan, V. V., Geetha, K., & Ramasubramanian, N. (2017). Design of RSA processor for concurrent cryptographic transformations. Microelectronics Journal, 63, 112-122.
27. Huo, Y., & Liu, D. (2018). High-throughput bit processor for cryptography, error correction, and error detection. Microprocessors and Microsystems, 61, 207-216.
28. Shaomeng Li, Jim Torresen, Oddvar Sørasen, "Improving a Network Security System by Reconfigurable Hardware," Department of Informatics, University of Oslo, Norway, 2004.
29. Deepthi Barbara Nickolas, Mr. A. Sivasankar, "Design of FPGA Based Encryption Algorithm using KECCAK Hashing Functions," International Journal of Engineering Trends and Technology (IJETT), Vol. 4, Issue 6, June 2013.
30. John Villasenor, William H. Mangione-Smith, "Configurable Computing," Department of Electrical Engineering, University of California, Los Angles, 1999.
31. Ashwini R. Tonde, Akshay P. Dhande, "Review paper on FPGA based Implementation of Advanced Encryption Standard (AES) algorithm," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2014.
32. T. Scheller and E. Kuhn, "Usability Evaluation of Configuration-Based ¨ API Design Concepts," in Human Factors in Computing and Informatics. Springer Berlin Heidelberg, 2013, pp. 54–73.
33. Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara, "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking", IJCSI International Journal of Computer Science Issues, vol. 8, no. 3, May 2011.
34. Askari, Nazanin et al. "An extended visual cryptography scheme without pixel expansion for halftone images." 2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (2013): 1-6.
35. Youmaran, Richard et al. "An Improved Visual Cryptography Scheme for Secret Hiding." 23rd Biennial Symposium on Communications, 2006 (2006): 340-343.

IX. AUTHORS PROFILE

V.Arun, Completed his M.Tech from JNTU Hyderabad and currently pursuing his Research degree at Reva University, Bengaluru. He is a Life member of ISTE . He has published his papers in reputed journals and conferences. His research areas are Cryptography, Embedded Systems, VLSI, and Communication Systems.

Dr. Rajashekhar C. Biradar has 29 years of teaching and research experience. He has many research publications in reputed national/international journals and conferences. Some of the journals where his research articles published are Elsevier, IET, Springer, Wiley and IOS Press, having good impact factors. He has published 55 papers in peer reviewed national and international journals, 62 papers in reputed national and international conferences and 3 book chapters. His Citations and h-index are Google Scholar, 844 citations (h-index = 15 and i-10index = 22), Scopus – 564 (h-index = 14), Web of Science – 369 (h-index=11). He is involved in research which covers various sorts of wireless networks such as ad hoc networks, sensor networks, mesh networks, network security, smart antennas, Index modulation, etc. He has guided 5 PhD's and currently, he is guiding 6 PhD students. He is a reviewer of various reputed journals and conferences and chaired many conferences. He is a Fellow IETE (FIETE) India, member IE (MIE) India, member ISTE (MISTE) India and senior member of IEEE (SMIEEE), USA
and member of IACSIT. He has been listed in Marquis' Who's Who in the World (2012 Edition), USA and Top 100 Engineers by IBC, UK. Interested Research Areas are Wireless Communication Systems, Communication Networks, Communication theory and systems.

Mahendra Vucha received his B. Tech in Electronics & Communication Engineering from JNTU, Hyderabad in 2007 and M. Tech degree in VLSI and Embedded System Design from MANIT, Bhopal in 2009. Completed his PhD from NIT Bhopal (M.P), India. His areas of interest are Hardware Software Co-Design, Cryptography, Analog Circuit design, Digital System Design and Embedded System Design. He is a life member of ISTE and IETE.