Ingénierie des Systèmes d'Information
Vol. 26, No. 3, June, 2021, pp. 329-335
Journal homepage: http://iieta.org/journals/isi

A Tabu Search Algorithm for General Threshold Visual Cryptography Schemes

Kanusu Srinivasa Rao[1*], Mandapati Sridhar[2]

[1] Dept. of Computer Science and Engineering, Acharya Nagarjuna University, Guntur 522510, India
[2] Dept. of Compute Applications, R.V.R. & J.C College of Engineering, Guntur 522019, India

Corresponding Author Email: kanususrinivas@yogivemanauniversity.ac.in

https://doi.org/10.18280/isi.260310

Received: 18 January 2021
Accepted: 10 May 2021

Keywords:
visual cryptography schemes (VCSs), visual secret sharing (VSS), pixels, images; shadows, contrast, probabilistic VSS (ProbVSS), tabu search (TS)

ABSTRACT

In Visual Cryptography Schemes (VCSs), for message n transparencies are generated, such that the original message is visible if any k of them are stacked. VCS especially for large values of k and n, the pixel expansion's reduction and enhancement of the recovered images' display quality continue to be critical issues. In addition to this, it is challenging to develop a practical and systematic approach to threshold VCSs. An optimization-based pixel-expansion-free threshold VCSs approach has been proposed for binary secret images' encryption. Along with contrast, blackness is also treated as a performance metric for assessing the recovered images' display quality. An ideally secure technique for a secret image's protection through its partition into shadow images (known as shadows) is the Visual Secret Sharing (VSS) scheme. Acquirement of a smaller shadow size or a higher contrast is the VSS schemes' latest focus. The white pixels' frequency has been utilized to demonstrate the recovered image's contrast in this work. While the Probabilistic VSS (ProbVSS) scheme is non-expansible, it can also be readily deployed depending upon the traditional VSS scheme. Initially, this work has defined the problem as a mathematical optimization model such that, while contingent on blackness and density-balance constraints, there is the maximization of the recovered images' contrast. Afterward, an algorithm dependent on the Tabu Search (TS) is devised in this work for this problem's resolution. Multiple complicated combinatorial problems have been successfully resolved with the powerful TS algorithm. Moreover, this work has attempted to bolster the contrast through the density-balance constraint's slight relaxation. Compared to the older techniques, the proposed optimization-based approach is superior regarding the recovered images' display quality and the pixel expansion factor from the experimental outcomes.

1. INTRODUCTION

Across the network, communication of critical and sensitive information like Quick Response (QR) images, medical images, medical reports, financial documents, and military maps. Secret Image's (SI) definition is given as real-time images that have confidential information. It is essential to consider security-related issues as digital services have swiftly and greatly progressed in this digital communication age. Especially in India, a Digital India is being made a reality through 462 million Indians endeavors. There is communication across the network of millions of information in the form of videos, audio, real-time images, and text. It signifies that security is, of course, a critical concern for this whole idea. At the time of SI communication, consideration of the SI's integrity, quality, and security is paramount. There is extensive utilization [1] of encryption/decryption and information hiding techniques for the SI's protection.

Human beings are inclined to preserve and protect important things, information or messages from potential loss or misuse. A lock and key system is used for storing items in safe places. Yet, there are two ways in which these items can be stolen. When the key is found, it could open to steal the items. Also, the system could be physically broken if the key is not found. A certain combinational key system has been developed to make the key more secure. This combinational key is shared between different people, or it is split into pieces (shares) that are kept at diverse locations. Must bring this distributed information back together, and key identification must occur to open the lock. At times, it is necessary to transfer the information from one place to another securely. It is quite necessary [2] to transmit this information through the preservation of its privacy.

The science of utilizing mathematics for data's encryption and decryption to keep the messages secure by modifying the data in an intelligible form (the plain text) into an unintelligible form (the ciphertext) is referred to as cryptography. Origins of the term cryptography have come from the Greek word "kryptós", which means "hidden", and from the word "gràphin", which means "writing". Hence, "hidden writing" is the cryptography term's correct meaning. This cryptosystem comprises the key, the ciphertext, the decryption algorithm, the encryption algorithm, and the plaintext. The plaintext will comprise of data or message that is readable and also normal. There is a key's utilization by encryption for the conversion of this plaintext into its ciphertext. The ciphertext is encrypted through the application of an encryption key on the plaintext. The process of decryption will retrieve the plaintext from its ciphertext. The cryptosystem (the cipher system) is controlled by a key that is only known by either the sender or the receiver. Such data are made secure with this very powerful cryptography.

Additionally, cryptanalysts can successfully break ciphers to acquire plaintext [3] from analysis of the cipher's contents.

As a security technique, Visual Cryptography (VC) will perform image encryption such that there is visual decryption of the original Image. This technique will randomly expand a secret image onto multiple visual key images. A share is a term used for each visual key Image. These visual key images are generally printed on transparent sheets, and there is visual decoding of the secret Image when there is an overlapping of a qualified subset of the keys. An example of VC with two visual keys is displayed in Figure 1. No information related to the secret Image is extracted when there is only a single individual visual key in VC. Even though there is the secret Image's display after the overlapping of multiple visual keys, there is no direct observation of each key from the overlapped outcome. The secret Image, as well as the visual keys, are safeguarded as being invisible to unauthorized users [4] for diverse security applications.

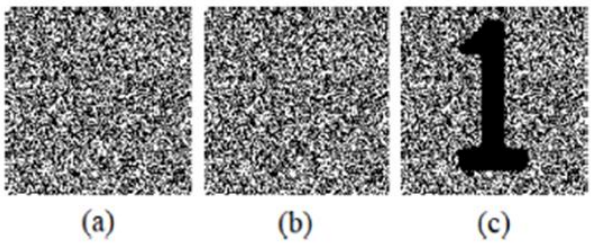

Figure 1. Example of VC: (a) visual key 1, (b) visual key 2, (c) Visually decoded secret image when the two visual keys printed on transparent sheets are overlapped

The VC utilizes two clear-cut pictures. While the first picture comprises random or noisy pixels, the second picture comprises secret data. The secret data's recovery from encrypted pictures is essentially tough. For the data's revelation, it is necessary to utilize the layers and the transparent pictures. Printing of the two layers onto a single transparent sheet is the simplest VC implementation. The VS's benefit is its ability to furnish computation problems when decoding and re-establish the secret image through stacking activity. With this property, the VC is specifically valuable for the low computation strategy [5]. Presentation of the VC technique was done in 1994 by Naor and Shamir. This secret imparting scheme offers greater security for a binary image. During the human vision, this scheme's legitimate deciphering is another benefit. VC strategies have numerous levels. For example, Colour images, gray images, and binary images are utilized for the VC's implementation. As per Naor and Shamir, an edge Visual Cryptography Scheme (VCS) can encode a provided secret picture into n shadow pictures (shares), in which any k or a greater amount of them can visually recover the secret image, but any or a lesser amount of them are unable to recover the secret image [6]. This scheme misuses the human visual framework for reading a secret message from some overlapping shares function; it will overcome the traditional cryptography's requirement for complex computations. Naor and Shamir gave the VC's elemental model for application in diverse applications with its incorporation of visual authentication, data hiding, etc. However, the model concept is why the complete restriction of these applications to the binary images' utilization. There is a drastic decrease in VC's applicability as binary images are generally restricted to text message representations.

For VCs, this work has proposed the ProbVSS and TS algorithm. The organization of the investigation is provided in the subsequent sections. Associated works in literature have been overviewed in Section Two. Diverse, utilized methods have been detailed in Section Three. The experimentations have been discussed in Section Four, and this work is concluded in Section Five.

2. LITERATURE SURVEY

Colour image conversion Halftone VC uses halftoning techniques for converting the color image into binary images. Consideration of the challenge of encoding color images into n shares of meaningful halftone images was done by Thomas and Charge [7]. Error Diffusion (ED) and Direct Binary Search (DBS) are the utilized halftone techniques by which a color image's secret pixel is encoded into shares. There is a comparison of these two methods depending upon Structural Similarity (SSIM), Universal Quality Index (AQI), Correlation, and Peak to Signal Noise ratio (PSNR).

A secret sharing scheme for visual information such as videos and images are called the VCS. From the origin of VCS itself, Progressive VCS (PVCS), extended VCS, *k* out of *n* VCS, etc., are the various revisions performed on the original VCS. Management of noise-like random shares, poor reconstruction accuracy, poor contrast of share images constructed, and pixel expansion are the various VCs' few frequent problems. Bhagate and Kulkarni [8] put forward the Improved Extended PVCS (IEPVCS) for these issues management, this approach does have to go through the cheating problem with VCS. The introduction of fake shares in the system and their impact on the secret information's reconstruction is the frequently employed approach for cheating with VCS. However, there are only a few VCS's which handle cheating through the introduction of fake shares.

The Homomorphic Visual Cryptographic Scheme (HVCS) proposal was provided by Yan et al. [9]. Good features of the standard VCS, like a loss-tolerance (as an example, the threshold) and the simply reconstructed method, wherein the secret image's decryption is dependent on the Human Visual System (HVS) without any cryptographic computation, have been inherited by the proposed HVCS. Moreover, Signal Processing in the Encrypted Domain (SPED) is supported by this scheme, for example, homomorphic operations and authentication that safeguard the user's privacy and offer security enhancement in particular applications computing, etc. The proposed HVCS' security and effectivity are demonstrated from the theoretical analysis and the simulation outcomes.

A-VCS was proposed by Li et al. [10] for sharing one or two secret images into three shadows by stacking any two shadows to reveal the secret image. Times the secret image is the shadow size. The exposed image's contrast is when one secret image has been shared. On the other hand, is the exposed image's contrast when two secret images have been shared. This work can also reveal the secret image with an *XOR* decoding operation and further enhance the exposed image's visual quality. With the *XOR* decoding operation, the exposed image's contrast is when one secret image is shared, and 1 is the exposed image's contrast when two secret images are shared. There is no distortion of the exposed two secret images, for instance, when two secret images are shared. The practicability and benefits of the proposed -VCS have been verified from the theoretical analyses and the experimental outcomes.

Two encryption approaches were proposed by Chiu and Lee [11] for the user-Friendly Progressive VC Schemes' (FPVCSs) construction. While the first approach is a generic OR-based FPVCS known as -FPVCS, the second approach is an *XOR*-based FPVCS known as -XFPVCS. (1) Systematic approaches, (2) the pixel-expansion's avoidance, (3) provision of meaningful shares with adjustable visual quality, and (4) elimination of the cover images' residual traces, are the two proposed models' prevalent issues. The work has also theoretically analyzed and executed experimentations to verify these proposed two models' visual quality. It is evident from the experimental outcomes that these proposed models do the simultaneous achievement of these goals. Moreover, with the parameter setting, the trace-elimination threshold is adjusted by -FPVCS to boost the proposed model's flexibility. -XFPVCS obtains a final recovered image that is fully decrypted.

The latest robust image watermarking algorithm, which was dependent on block classification and VC, was presented by Fatahbeygi and Tab [12]. There is the original image's decomposition into non-overlapping blocks at this proposed algorithm's commencement. Later, these blocks' categorization as non-smooth and smooth classes is done by utilizing the Canny edge detection and the Support Vector Machine (SVM) classification approach. Can produce two image shares with the VC approach: A master share, which is built as per the outcomes of the block classification, and an owner share, which is produced through utilization of the master share along with a binary watermark. The retrieval of the watermark is done through the stacking of the master share and the owner share for verification of the image's owner. There is a substantial enhancement in the proposed watermarking algorithm's robustness through avoidance of blocks that are not robust against attacks. This algorithm is wholly imperceptible since it concealed the watermark pattern without the original host image's modification.

The introduction of a novel threshold secret image sharing scheme with two decoding options was done by Wu and Yang [13]. Offered Stacking-to-see decryption and lossless image reconstruction in this proposed scheme through a combination of the Color-Black-and-White VC Scheme (CBW-VCS) and the Polynomial-based Secret Image Sharing (PSIS). Initially, a general threshold CBW-VCS is supplied for the color shares' construction. There is a grayscale secret image's conversion into a p-radix image and a binary image. The PSIS does the encryption of the p-radix image under operation to obtain p-radix shadows. Afterward, color share construction was done by developing a color share generation algorithm with data embedding. The proposed scheme's benefits and effectivity are demonstrated by theoretical analysis as well as by adequate experimentations.

A novel two-level information protection scheme dependent on VC and QR code was designed by Fu et al. [14]. Public-level information is directly read out from the shares using any generic QR reader software or device. In addition to this, there is the decoding of the privacy-level information with three distinct decryptions suited for non-computation with a relative difference, lightweight computation with a relative difference, and common computation environments with relative difference 1. The proposed scheme retains the benefits of the QR code and VC. Thus, this scheme is distinct from other associated schemes that have a high payload, low robustness against deformations, and low complexity in computations. Theoretical verification of this proposed scheme's effectiveness has been confirmed. Analyses and simulation outcomes have proved the proposed scheme's protection ability for two-level information with multiple decryptions. Also, this scheme is found to have numerous benefits when compared with the earlier schemes.

Graphical password authentication was improved upon by Gulsezim et al. [15] with the Twofish Encryption and Visual Cryptography (TEVC) algorithm's utilization. There is an unpredictable organization of this proposed TEVC since it is much tougher to predict the correct graphical password and sort its particles into the appropriate order compared to the standard alphanumeric password system. JAVA platform has been utilized for TEVC's assessment. It is verified from the outcomes of the assessment that the proposed TEVC offers secure authentication. This algorithm has also been found to be more prudent and has lower complexity in time when compared against other common existing algorithms fingerprint scan with password and message code confirmation.

For a variation of each shadow's capability to display a secret image, the Weighted VCS (WVCS) permitted the dealer to allocate weight to each shadow (participant) as per the participant's priority. Low visual quality was a drawback of the earlier Weighted Random Grid-based VCS (WRGVCS). A novel WRGVCS for a (k, n) threshold was designed by Yan et al. [16] to improve the exposed secret image's image quality and realize more features. Features like no pixel expansion and no codebook design are accomplished with the Random Grids' (RG) usage. For the image quality's improvement, there is the enhancement of the probability of covering the valid bits. The designed scheme's effectivity is indicated from the simulated outcomes and the security analyses. There is a demonstration of the designed scheme's improvement over other relative weighted VCSs based on the contrast and feature comparisons. Decrease of the weighted effect for certain thresholds and the fact that the parameters do not directly derive the designed scheme's theoretical contrast are this work's constraints.

The research in literature section have shown some security problems. The transmitting and storing information in digital form is very important to ensure an adequate level of security of ciphers use. This research can increase the security of existing system by combining it with another encryption method.

3. METHODOLOGY

The difference between black's white pixel densities and the recovered images' white reconstruction areas constitute the basis of the contract's classical definition. In traditional VCS, contrast is often utilized for the measurement of the recovered images' display quality. There is a discussion about the ProbVSS and TS algorithm in this section.

3.1 Probabilistic Visual Secret Sharing (ProbVSS) Scheme

B_0 and B_1 are the two collections of $n \times m$ Boolean matrices which are used for a $(k;n)$ VSS Scheme's representation. When a white (resp. black) pixel is shared, there is random selection of a single row of the Boolean matrix B_0 (resp. B_1) to a relative shadow by the dealer. The gray level of the m subpixels in every one of the n shadows is the chosen matrix's definition. The validity of a VSS Scheme is dependent on the fulfillment [17] of the following conditions:

1. $H(V) \leq d - \alpha m\ (resp.(H(V) \geq d)$is fulfilled by the *"OR"*-ed V of any k of the n rows for any S in B_0 (resp. B_1).

2. For any subset$\{ i_1 ; i_2 ; \ldots i_q \}$ of $\{1; 2 \ldots ; n\}$ with $(q < k)$the two collections of $q \times m$ matrices which are gained from the restriction of each $n \times m$ matrix in B_0 to B_1, to rows $\{ i_1 ; i_2 ; \ldots i_q \}$ cannot be discerned as they comprise of similar matrices with similar frequencies.

Contrast is the term used for the first condition whereas, security is the term used for the second condition. Because of the security condition, if it does not have greater than k shadows, it would not be able to gain any information related to the shared secret.

The basic (2, 2) VSS scheme will stack two shadows for the shared secret's recovery such that the "black" will now be $2B0W$ while the "white" will now be $1B1W$, in which, $xByW$ will indicate that it has utilized x black sub pixels and y white sub-pixels for an original pixel's representation. Since each pixel's representation is given as $1B1W$ sub-pixels, the scheme is unable to obtain any information from any single shadow.

White set C_0 that containn_λ a matrix, and black set C_1 that contains $n_\gamma n \times 1$matrix are the two sets which provide the $(k;\ n)$ ProbVSS scheme's representation. When a white (resp. black) pixel is shared, the dealer will initially pick one$(n \times 1)$ column matrix in C_0 (resp.C_1) randomly, and later, will randomly pick a single row of this column matrix to a relative shadow. The colour level of pixel in every one of the n shadows is defined by this chosen matrix. Validity of a ProbVSS Scheme is based on the fulfilment of the below conditions:

1. The "*OR*" value of any k-tuple column vector V will be $L(V)$ for these n_λ (resp.n_γ) matrices in the set C_0 (resp. C_1). A set λ (resp. γ) is formed from these values of every matrices.

2. $p_0 \geq p_{TH}$, and $p_1 \leq p_{TH} - \alpha$ are satisfied by the two sets λ and γ, wherein, p_0 and p_1 are the appearance probabilities of the "0" (white color) in the respective sets λ and γ.

3. p_0 and p_1 will be similar for any subset $\{ i_1 ; i_2 ; \ldots ; i_q \}$ of $\{1;\ 2;\ \ldots ; n\}$ with $(q < k)$.

While the first two conditions are referred to as contrast, the third condition is referred to as condition security. Based on the earlier-mentioned definition, as matrices in C_0 and C_1 are $(n \times 1)$ matrices, the Pixel Expansion will also be one. However, as the traditional VSS scheme's B_0 and B_1 are $(n \times m)$ matrices, the Pixel Expansion will be m.

3.2 Tabu Search (TS) Algorithm

To maximize the contrast of recovered images, subject to density-balance constraints, Tabu Search is used to optimize this. Given k, n, and the blackness requirement, the proposed optimization-based threshold VCS model determines a set of choice probabilities. An extensive range of challenging combinatorial optimization problems can be resolved with the powerful solution technique known as TS. This local search technique is capable of avoidance of a local minimum or a cycle's repetition of a cycle through its combination with a variety of approaches. Glover gave the first introduction of the TS which exhibited huge effectivity in the resolution of tough optimization problems. TS will utilize an evaluation function for retaining the solution, which can enhance the f value (which is picked from a set of neighboring solutions N(s)) such that there is the existing solution's [18] replacement with a chosen best neighbor at every iteration.

The TS's primary characterization is given as a Tabu List T (memory) that is made up of the last solutions visited but does not provide the possibility of a solution which has already been accepted and stored in the Tabu List. Long-term memory and short-term memory are the TS's two utilized types of memory. An aspersion criterion is utilized for the long-term memory's execution. This type of memory will permit a Tabu move's performance despite its Tabu classification. While short-term memory is associated with a Tabu List structure, it does contain a list of temporary forbidden moves such that there is avoidance of visit to an already explored solution.

The following points form the basis [19] for the TS:

- Utilization of the flexible memory structures (short, medium, and long term) that facilitates the complete exploration of the evaluation criteria as well as the search history.
- A control mechanism that is reliant on alternation between the search process's conditions, which constrict (restriction Tabu), and the conditions which liberate (aspiration criterion).
- Incorporation of the search's strategies of intensification and diversification:
    - The medium-term memory's utilization and strengthening of the search in the regions of the newly found best solutions are done by the intensification strategy.
    - The long-term memory's utilization and searching of the new regions are done by the diversification strategy.

3.3 General Algorithm of TS

TS's general algorithm is presented below:

1) Acquisition of an initial solution (initialization).

2) Creation of a list of candidates' movements.

3) The best candidate's selection. Tabu restrictions and the aspiration criteria form the basis of this selection.

This will offer an alternative that would not be registered only if it is found to be better in comparison to the earlier solution.

4) The stopping criterion's application.

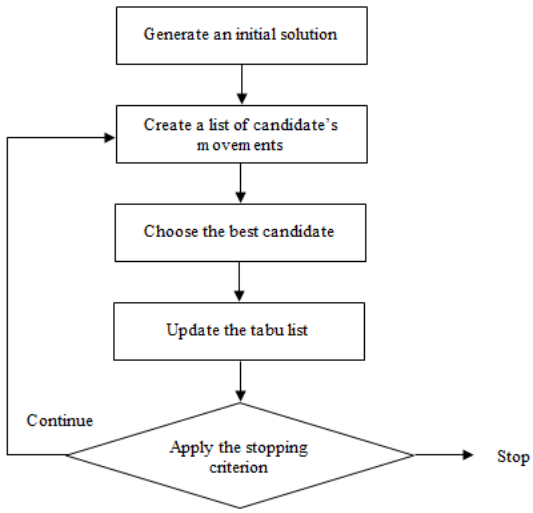

Figure 2. Flowchart for Tabu search method

Continue: Modification of the candidates of eligibility (Tabu restriction and aspiration criterion). Move back to 2.

Stop: Proceed towards the strategies of intensification and diversification.

Figure 2 illustrates the TS method's flowchart.

4. RESULT AND DISCUSSION

In this section, the probVSS and Tabu methods are used. Experiments are carried out using $(k, n \; and \; k = 5, n)$ for different blackness range (100 to 70). Table 1 shows the parameters of Tabu Search. The contrast (various blackness range) as shown in Tables 2 to 6 and Figures 3 to 8.

Table 1. Parameters of Tabu search

Parameters	Value
Number of neighbourhoods	500
Local search around neighborhood	500
Tabu list size	100
Tabu criteria	0.03

Table 2. Contrast for Tabu blackness of range (100, 90)

(*k*,*n*) for different Blackness Range (100,90)	ProbVSS	Tabu
(2, 3)	33.5	34.2
(2, 4)	29.4	30.1
(2, 5)	28.8	29.4
(2, 6)	27.9	28.6
(2, 7)	25.7	26.4
(2, 8)	25.6	26.2

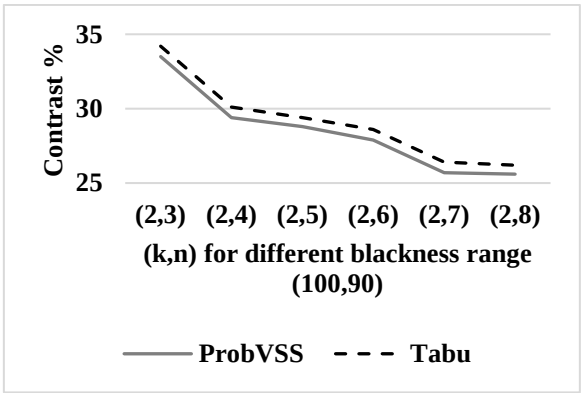

Figure 3. Contrast for Tabu blackness of range (100, 90)

From the Figure 3, it can be observed that the Tabu has higher contrast by 2.06% for (2, 3) blackness range (100, 90), by 2.35% for (2, 4) blackness range (100, 90), by 2.06% for (2, 5) blackness range (100, 90), by 2.47% for (2, 6) blackness range (100, 90), by 2.68% for (2, 7) blackness range (100, 90), and by 2.32% for (2, 8) blackness range (100, 90) when compared with probVSS respectively.

Table 3. Contrast for Tabu blackness of range (90, 80)

(*k*,*n*) for different Blackness Range (90,80)	ProbVSS	Tabu
(2, 3)	34.4	35.4
(2, 4)	30.3	31.2
(2, 5)	29.7	30.4
(2, 6)	29	29.6
(2, 7)	26.8	27.4
(2, 8)	26.6	27.2

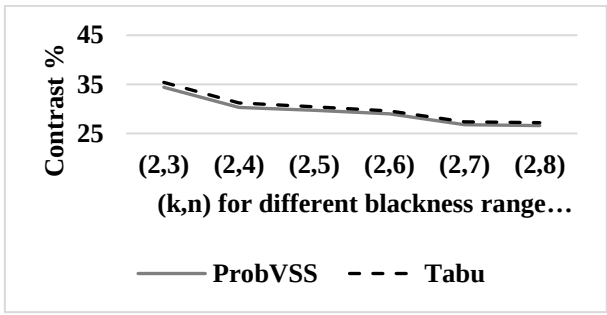

Figure 4. Contrast for Tabu blackness of range (90, 80)

From the Figure 4, it can be observed that the Tabu has higher contrast by 2.86% for (2, 3) blackness range (90, 80), by 2.92% for (2, 4) blackness range (90, 80), by 2.32% for (2, 5) blackness range (90, 80), by 2.04% for (2, 6) blackness range (90, 80), by 2.21% for (2, 7) blackness range (90, 80), and by 2.23% for (2, 8) blackness range (90, 80) when compared with probVSS respectively.

Table 4. Contrast for Tabu blackness of range (80, 70)

(*k*,*n*) for different Blackness Range (80,70)	ProbVSS	Tabu
(2, 3)	35.7	36.6
(2, 4)	31.6	32.3
(2, 5)	30.4	31.3
(2, 6)	29.9	30.6
(2, 7)	27.5	28.2
(2, 8)	27.4	28

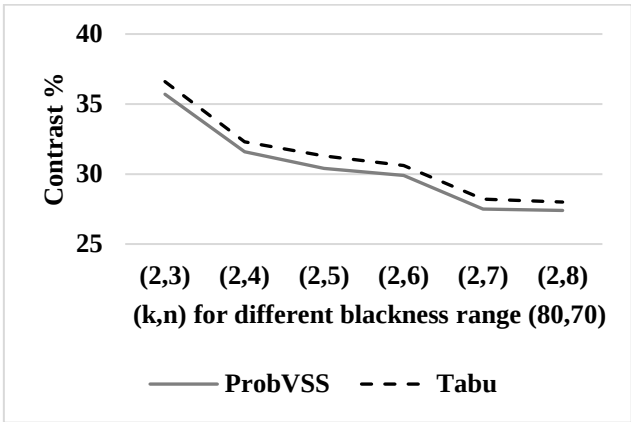

Figure 5. Contrast for Tabu blackness of range (80, 70)

From the Figure 5, it can be observed that the Tabu has higher contrast by 2.48% for (2, 3) blackness range (80, 70), by 2.19% for (2, 4) blackness range (80, 70), by 2.91% for (2, 5) blackness range (80, 70), by 2.31% for (2, 6) blackness range (80, 70), by 2.51% for (2, 7) blackness range (80, 70), and by 2.16% for (2, 8) blackness range (80, 70) when compared with probVSS respectively.

Table 5. Contrast for Tabu blackness of range (100, 90)

(*k*=5,*n*) for different Blackness Range (100, 90)	ProbVSS	Tabu
(2, 5)	28.8	29.4
(3, 5)	19.2	19.8
(4, 5)	12.7	13.2

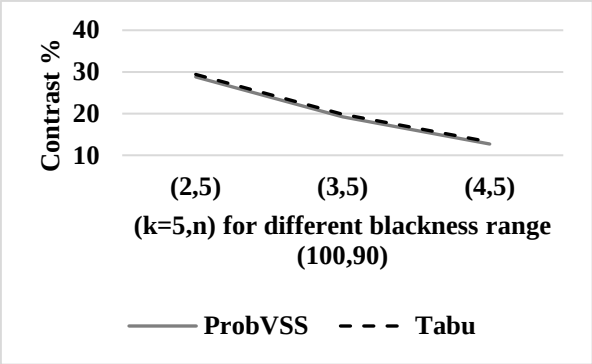

Figure 6. Contrast for Tabu blackness of range (100, 90)

From the Figure 6, it can be observed that the Tabu has higher contrast by 2.06% for (2, 5) blackness range (100, 90), by 3.07% for (3, 5) blackness range (100, 90) and by 3.86% for (4, 5) blackness range (100, 90) when compared with probVSS respectively.

Table 6. Contrast for Tabu blackness of range (90, 80)

(*k*=5,*n*) for different Blackness Range (90,80)	ProbVSS	Tabu
(2, 5)	29.7	30.4
(3, 5)	20.6	21.2
(4, 5)	13.5	15.1

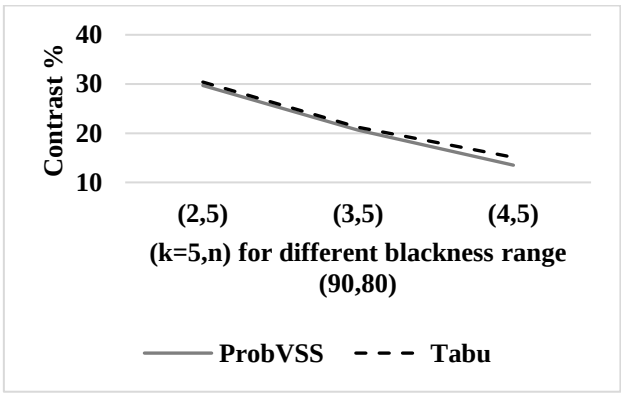

Figure 7. Contrast for Tabu blackness of range (90, 80)

Table 7. Contrast for Tabu blackness of range (80, 70)

(*k*=5,*n*) for different Blackness Range (80,70)	ProbVSS	Tabu
(2, 5)	30.4	31.3
(3, 5)	20.8	21.4
(4, 5)	13.6	14.3

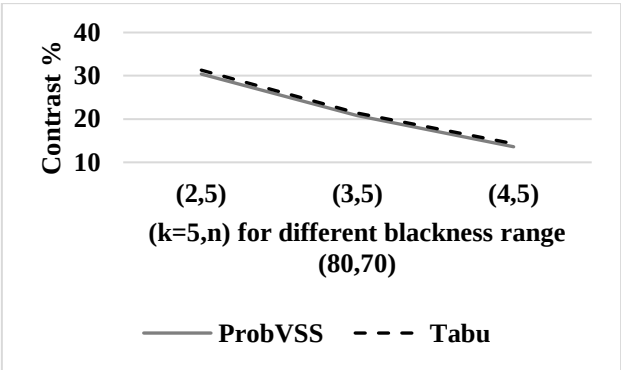

Figure 8. Contrast for Tabu blackness of range (80, 70)

Table 7 represents blackness of range (90, 80). From the Figure 7, it can be observed that the Tabu has higher contrast by 2.33% for (2, 5) blackness range (90, 80), by 2.87% for (3, 5) blackness range (90, 80) and by 11.19% for (4, 5) blackness range (90, 80) when compared with probVSS respectively.

From the Figure 8, it can be observed that the Tabu has higher contrast by 2.92% for (2, 5) blackness range (80, 70), by 2.84% for (3, 5) blackness range (80, 70), and by 5.02% for (4, 5) blackness range (80, 70) when compared with probVSS respectively.

5. CONCLUSION

As a cryptographic strategy, VC allows the encoding of visual data such that the human visual system can carry out the decryption without any computer guidance. To manage the issue of binary secret images' general threshold VC, this work has proposed a new approach based on optimization. Probabilistic technique-based novel (k; n) ProbVSS schemes with non-expansible shadow size are presented in this work. The similarity in the sizes of the original images as well as shadows are defined by the term non-expansible. Distinction of the recovered image's contrast by the visual system depending on the difference of the white colour's frequency in black and white areas is highlighted by the term "probabilistic". TS is a novel metaheuristic that is extremely effective as it is able to resolve an extensive problem range. Presentation of the metaheuristic "TS" cryptography's first adaptation was given in this work. The proposed algorithm utilizes Variable-length encoding for the data input's symbolic representation in order to permit the encryption of any type of information (sound, image, text, and so on). A secret key referred to as the "Tabu-key" is produced by the system. Efficiency and resistance capability towards brute-force attacks are this key's fundamental attributes. Outcomes have demonstrated that, when compared with the ProbVSS, the Tabu has higher contrast by 2.06% for (2, 3) blackness range (100, 90), by 2.35% for (2, 4) blackness range (100, 90), by 2.06% for (2, 5) blackness range (100, 90), by 2.47% for (2, 6) blackness range (100, 90), by 2.68% for (2, 7) blackness range (100, 90), and by 2.32% for (2, 8) blackness range (100, 90). Furthermore, upon comparison with the ProbVSS, the Tabu has higher contrast by 2.06% for (2, 5) blackness range (100, 90), by 3.07% for (3, 5) blackness range (100, 90), and by 3.86% for (4, 5) blackness range (100, 90). In future, hybrid halftoning of pulse width modulators can be used to produce better results.

REFERENCES

[1] Mary, G.S., Kumar, S.M. (2020). Secure grayscale image communication using significant visual cryptography scheme in real time applications. Multimedia Tools and Applications, 79(15): 10363-10382. https://doi.org/10.1007/s11042-019-7202-7

[2] Bhat, M.N., Buradagunta, S., Rani, K.U. (2019). A novel approach to key management using visual cryptography. Ingénierie des Systèmes d'Information, 24(6): 627-632. https://doi.org/10.18280/isi.240610

[3] Gurunathan, K., Rajagopalan, S.P. (2020). A stegano-visual cryptography technique for multimedia security. Multimedia Tools and Applications, 79(5): 3893-3911.

https://doi.org/10.1007/s11042-019-7471-1
[4] Jiao, S., Feng, J., Gao, Y., Lei, T., Yuan, X. (2020). Visual cryptography in single-pixel imaging. Optics Express, 28(5): 7301-7313. https://doi.org/10.1364/OE.383240
[5] Divya, K., Padmaja, N. (2019). Password processing techniques using visual cryptography and optical character recognition. Journal of the Gujarat Research Society, 21(16): 2459-2467.
[6] Li, P., Yin, L., Ma, J. (2020). Visual cryptography scheme with essential participants. Mathematics, 8(5): 838. https://doi.org/10.3390/math8050838
[7] Thomas, S.A., Gharge, S. (2020). Halftone visual cryptography for color images using error diffusion and direct binary search. In Emerging Trends in Photonics, Signal Processing and Communication Engineering, 99-105. https://doi.org/10.1109/ICOEI.2018.8553863
[8] Bhagate, S.B., Kulkarni, P.J. (2020). Cheating prevention in improved extended progressive visual cryptography scheme. In Computing in Engineering and Technology, 585-595. https://doi.org/10.1007/978-981-32-9515-55
[9] Yan, X., Lu, Y., Liu, L., Wan, S., Ding, W., Liu, H. (2020). Exploiting the homomorphic property of visual cryptography. In Cryptography: Breakthroughs in Research and Practice, 416-427.
[10] Li, P., Ma, J., Yin, L., Ma, Q. (2020). A construction method of (2, 3) visual cryptography scheme. IEEE Access, 8: 32840-32849. https://doi.org/10.1109/ACCESS.2020.2973659
[11] Chiu, P.L., Lee, K.H. (2019). Efficient constructions for progressive visual cryptography with meaningful shares. Signal Processing, 165: 233-249. https://doi.org/10.1016/j.sigpro.2019.06.038
[12] Fatahbeygi, A., Tab, F.A. (2019). A highly robust and secure image watermarking based on classification and visual cryptography. Journal of Information Security and Applications, 45: 71-78. https://doi.org/10.1016/j.jisa.2019.01.005
[13] Wu, X., Yang, C.N. (2019). A combination of color-black-and-white visual cryptography and polynomial based secret image sharing. Journal of Visual Communication and Image Representation, 61: 74-84. https://doi.org/10.1016/j.jvcir.2019.03.020
[14] Fu, Z., Cheng, Y., Liu, S., Yu, B. (2019). A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions. Measurement, 141: 267-276. https://doi.org/10.1016/j.measurement.2019.03.080
[15] Gulsezim, D., Zhansaya, S., Razaque, A., Ramina, Y., Amsaad, F., Almiani, M., Oun, A. (2019). Two factor authentication using Twofish encryption and visual cryptography algorithms for secure data communication. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 405-411. https://doi.org/10.1109/IOTSMS48152.2019.8939261
[16] Yan, X., Liu, F., Yan, W.Q., Yang, G., Lu, Y. (2020). Weighted visual cryptographic scheme with improved image quality. Multimedia Tools and Applications, 1-16. https://doi.org/10.1007/s11042-020-08970-y
[17] Yang, C.N. (2004). New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters, 25(4): 481-494. https://doi.org/10.1016/j.patrec.2003.12.011
[18] Douiri, S.M., Elbernoussi, S. (2017). A steganographic method using tabu search approach. In 2017 Sixteenth Mexican International Conference on Artificial Intelligence (MICAI), pp. 30-33. https://doi.org/10.1109/MICAI-2017.2017.00013
[19] Kaddouri, Z., Omary, F. (2017). Application of the tabu search algorithm to cryptography. International Journal of Advanced Computer Science and Applications, 8(7): 82-87. https://doi.org/10.14569/IJACSA.2017.080712