International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

# NEW FRAMEWORK FOR REVERSIBLE DATA HIDING IN ENCRYPTED DOMAIN

**G.Swathi [1],Mr. A. Ranjith Kumar [2].**

*[1]pursuing M.Tech (CSE), [2]working as an Assistant Professor CSE, Sree Visvesvaraya Institute of Technology & Science, Chowdarpalle, Devarkadra (Md), Mahabubnagar (D), Telangana, Affiliated to JNTUH, (India)*

**ABSTRACT:**

*In the secret word more than you quit offering on that one decade, hundreds from claiming reversible data hiding (RDH) algorithms have been accounted through exploring the connection the middle of the neighboring pixels (or coefficients), additional data might a chance to be installed under the group picture reversibly. However, these RDH algorithms cannot be accomplished in encrypted domain directly since the correlation between the neighboring pixels will disappear after encryption. In order to accomplish RDH in encrypted domain, specific RDH schemes have been designed according to the encryption algorithm utilized. In this paper, we recommend another straightforward yet compelling structure to RDH for encrypted area. In the suggested framework, those pixels Previously, a plain picture would firstly isolated under sub-blocks for the size about* $m \times n$. *Then with an encryption key, a key stream (a stream of random or pseudorandom bits/bytes that are combined with a plaintext message to produce the encrypted message) is generated, and the pixels in the same sub-block are encrypted with the same key stream byte. After the stream encryption, the encrypted* $m \times n$ *sub-blocks are randomly permutated with a permutation key. Since the correspondence the middle of those neighboring pixels in every sub-block could be well safeguarded in the encrypted domain, the vast majority for the individuals a while ago recommended RDH schemes might be connected of the encrypted picture specifically. A standout amongst the primary merits of the recommended skeleton may be that the RDH plan may be free of the picture encryption algorithm. That is, the server manager (or channel administrator) does not need to design a new RDH scheme according to the encryption algorithm that has been conducted by the content owner; instead, he/she can accomplish the data hiding by applying the numerous RDH algorithms previously proposed to the encrypted domain directly.RDH (reversible data hiding )in plain domain aims at developing a method*

*that increase the embedding capacity as high as possible while keeping the distortion as low as possible.*

## I. INTRODUCTION

Reversible data hiding (RDH) can imperceptibly hide data into digital images, and more importantly, the original image can be reconstructed completely after the embedded data have been extracted out. As a special case of information hiding, RDH can find many applications. Its reversibility may be particularly alluring At genuine inconsistency devotion may be needed, e. g for medicinal and military image transforming. The classical RDH schemes have been proposed based on three fundamental strategies: lossless compression, difference expansion (DE), histogram shifting (HS). Almost all of today's RDH methods are derived from these three strategies. Among them, the HS based methods have attracted much attention. They can also be divided into three different approaches, *i.e.*, (original) histogram shifting (HS), difference histogram shifting (DHS), and prediction-error histogram shifting (PEHS). Nowadays, DHS and PEHS based methods have received much more attention because of their large embedding capacity and high fidelity. Numerous DHS and PEHS based algorithms were proposed in the past few years. For these two advanced approaches, the Fundamental perfect will be to investigate the correspondence between the neighboring pixels in a group image, Furthermore hence An Contrast or prediction lapse histogram for higher peaks might make created. Then those extra message might a chance to be reversibly inserted under the host picture by means of modifying the Contrast histogram alternately prediction lapse histogram.

As the era of cloud computing is coming, RDH in encrypted domain attracts more and more attention. A content owner may not trust the server manager (or channel administrator), and he/she will encrypt the image first and then upload it to the server. During the server end, the capacity should control those encrypted information same time guaranteeing the plain content's integument is seriously desired, e. g , a portion extra information necessities to be stowed away under these encrypted pictures should Stamp their ownership, What's more Then the plain content could be restored totally..

In data are appended by flipping three least significant bits (LSBs) of encrypted image and extracted with the aid of spatial correlation in natural image. The error rate of extracted bits was further decreased by Hong *et al.* with an improved measurement of smoothness and a new side match scheme. In both the appended data can only be extracted after image decryption. In other words, a receiver having data-hiding key but no content owner key cannot extract any information. To overcome this problem, a separable reversible data-hiding scheme is proposed, in which the LSBs of the encrypted image is compressed by a specific strategy (*i.e.*, finding the syndromes of a low-density parity check matrix to compress the LSBs of the encrypted image) designed for encrypted data, and then an extra space is created to append the additional data.

In Qian and Zhang further improved the embedding capacity of the scheme via using distributed source coding. The separable reversible data-hiding methods in try to space out room from the encrypted image directly which follows the idea of compressing the encrypted image. However, lossless vacating space from the encrypted picture will be troublesome Furthermore accordingly for A percentage condition the extra information might not

a chance to be concentrated precisely and the first picture can't be recouped totally. Considering this issue, Ma *et al*. and Zhang *et al*. proposed some new methods to improve the performance by reversing the order of encryption and vacating room. In the light of this idea, they empty out room prior to image encryption by shifting the histogram of estimating errors of some pixels, and the emptied out rooms are used for data hiding. In addition, according to the coding/decoding principle of the joint photographic expert group (JPEG) image, a specific RDH algorithm [20] was proposed for the encrypted JPEG image by Qian and Zhang *et al*. Looking at all of the aforementioned schemes, it becomes clear that the RDH algorithms in the encrypted domain are designed specifically. Those various RDH strategies formerly recommended in the plain area can't be connected of the encrypted picture directly, since in the superbly encrypted domain, those correspondence the middle of those neighboring pixels/coefficients doesn't exist any longer. Without utilizing those correspondence the middle of those neighboring pixels/coefficients, those RDH routines recommended in the plain area can't a chance to be effectively actualized. In this paper, we recommend another structure to RDH done encrypted Web-domain. By means of another encryption strategy, the relationship the middle of the neighboring pixels could a chance to be safeguarded great over encrypted Web-domain. In there will be no need should particularly outline the RDH plan in the encrypted Web-domain. With respect to contrary, various RDH schemes formerly outlined in non-encrypted Web-domain could be connected with our suggested schema straightforwardly to manifestation the RDH clinched alongside encrypted area. The rest of this paper is organized as follows. In Section II, a new framework for RDH in encrypted domain is introduced. We show that in our framework some statistical characteristics are preserved via using our specific encryption algorithm, and thus numerous RDH algorithms previously proposed can be accomplished in encrypted domain directly.

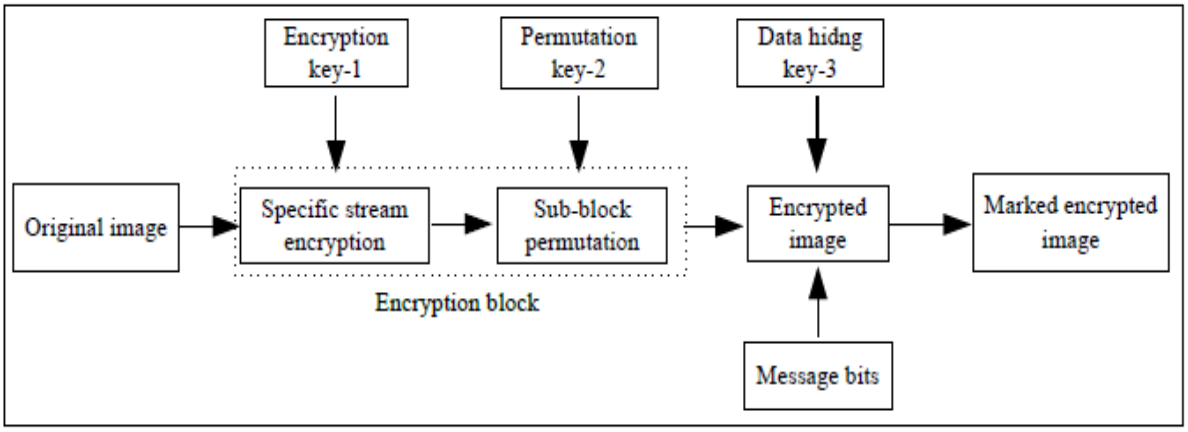
## II.EXISTING SYSTEM

The several RDH techniques formerly proposed in the simple domain can't be implemented to the encrypted photo directly, since in the perfectly encrypted area, the correlation between the neighboring pixels/coefficients does no longer exist anymore. Without the use of the correlation between the neighboring pixels/coefficients, the RDH techniques proposed in the simple domain can't be effectively applied.

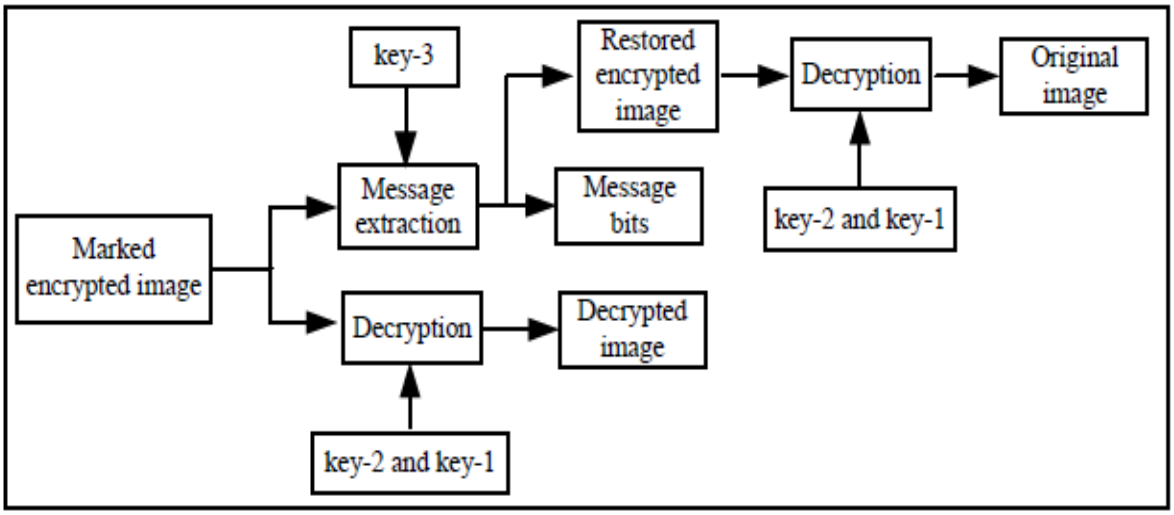
## III.SYSTEM ARCTECHTURE

Designing is the maximum essential phase. The Design procedure includes growing a conceptual view of the system, setting up gadget structure, figuring out information string and facts stores, decomposing high degree capabilities into sub-features, setting up relationships, interconnections among additives and growing concrete information illustration.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354




(a)




(b)

Fig. 1. The block diagram of our proposed framework. (a) data hiding process. (b) data extraction and image restoration.

In the sending end, those plain picture is firstly isolated under sub-blocks. Then, through a particular stream cipher, those partitioned picture is encrypted with those encryption magic key-1. Following that, those sub-blocks of the stream encrypted picture are permutated for the permutable magic key-2, and the encrypted picture is acquired.. Additional data are reversibly embedded into the encrypted image by the server manager (or channel administrator) with the data hiding key *key*-3. Note that in our framework, the RDH scheme selected for data hiding can be any of the previously proposed DHS or PEHS based approaches. The flow chart is presented in Figure 1(a).

In the receiving end, there are two cases. In the first case, the receiver will decrypt the image with the decryption keys (*i.e.*, *key*-2 and *key*-1) directly, and the decrypted image is similar to the original host image. In the second case, firstly the additional hidden data is extracted and meanwhile the encrypted image is reversibly recovered with data hiding *key*-3. Then the adequate encrypted angel is decrypted to access the aboriginal host angel with the decryption keys (i.e., key-2 and key-1).The encryption algorithm used in our framework includes two steps: specific stream encryption and permutation.

## III. SPECIFIC STREAM ENCRYPTION

Preceding encryption, the plain picture i may be isolated under $N$ non-overlapping sub-blocks $\{B1,B2,\ldots,BN\}$. Those sub Squares $\{B1,B2,\ldots,BN\}$ are with the span for $m\times n$ and scanned in the order from left to right and then top to bottom. Let by $Pi,j(1\leq i\leq N,1\leq j\leq m\times n)$ denotes one of the pixels in sub-block $Bi$, where $i$ represents the index of a sub-block, and $j$ represents the index of the pixel in the sub-block $Bi$. In each sub-block, the pixels are also scanned from left to right and then top to bottom.

Without loss of generality, we assume that in the plain image, each pixel is represented with eight bits. Any bit in the pixel $Pi,j$ can be represented by $pi,j,k(1\leq i\leq N,1\leq j\leq m\times n,1\leq k\leq 8)$, where $i$ represents the index of the sub-block $Bi$, $j$ represents the index of the pixel in the sub-block, and $k$ represents that $pi,j,k$ is the $k$th bit of $Pi,j$. The pixel value can be represented by $Pi,j=\Sigma pi,j,k\times 2k-18k=1$ (1)

According to the encryption *key*-1, run the stream cipher to generate the key stream with the length of $N$ bytes (*i.e.*, $N\times 8$ bits). For simplicity, each byte of the generated key stream are called **key stream byte** in the following. We represent the key stream byte with $Ri(1\leq i\leq N)$, where $i$ is the index of the generated key stream bytes. Since each key stream byte has eight bits, any bit in one key stream byte can be represented by$ri,k(1\leq i\leq N,1\leq k\leq 8)$, where $i$ represents the index of the key stream bytes, and $k$ represents that $ri,k$ is the $k$th bit of $Ri$. The generated key stream byte can be represented $Ri=\Sigma ri,k\times 2k-18k=1$ (2) In encryption phase, the bitwise exclusive-or (XOR) operation is performed between $Pi,j$ and $Ri$, as shown in Eq.(3). $Ei,j=Pi,j \wedge Ri$ $(1\leq j\leq m\times n)$ (3)

The place ^ speaks to the spot insightful XOR operation. Note that for eq. (3), every last one of pixels $\{Pi,1,Pi,2,\ldots,Pi,m\times n\}$ in the i th sub-block need aid encrypted with those same enter stream byte $Ri$. The obtained encrypted pixel $Ei,j$ also has eight bits. It can be represented by $Ei,j=\Sigma ei,j,k\times 2k-18k=1$ (4)

## IV. PERMUTATION

Permute all the stream encrypted sub-blocks with encryption key *key*-2. We can get the permutated image. Note that in this step, we main upset the request of the sub-blocks, and the request of the pixels inside each sub-block may be even now safeguarded. How will apply RDH calculation should Our Framework: in the encrypted image, the higher focuses (situated during 0 and ±1) of the Contrast histogram alternately prediction lapse histogram even now exist, What's more accordingly RDH calculations could effortlessly be refined in the encrypted area. Without misfortune of generality, we separate the encrypted picture under sub-blocks, and the pixel in the encrypted picture may be quell Toward $Ci,j(1\leq i\leq NE,1\leq j\leq mE\times nE)$, the place $NE$ speaks to those

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

amount of sub-blocks, and the span of the sub-block may be spoken to Toward $mE \times nE$. To avoid the saturation (*i.e.*, the overflow or underflow) during the embedding process, the saturated pixels (pixels with value 0 or 255) have to be preprocessed by modifying one grayscale unit and noted in a location map $L$ (initialized to be empty) as that in [21]. To do this, visit pixels sequentially and append a bit "0" to $L$ when $Ci,j \in \{1,254\}$. If $Ci,j \in \{0, 255\}$, append a bit "1" to $L$ and modify $Ci,j$ to $Ci,j\,'$ using the following equation

$Ci,j\,' = \{254\ if\ Ci,j = 255\ 1\ if\ Ci,j = 0\ Ci,j\ otherwise$ (8)

The length of $L$ is equal to the number of pixels with values 0, 1, 254 and 255 in the encrypted image. As seen, after overflow or underflow processing, a new image whose pixels are in the range [1, 254] is obtained. The area map l and the extra message both ought further bolstering be installed under those encrypted picture. Those encrypted pictures with 1×2, 2×2, 3×3 sub-blocks need aid exemplified On fig. 2. Those are a guide l What's more extra message will make inserted under encrypted area through modifying the distinction histogram.

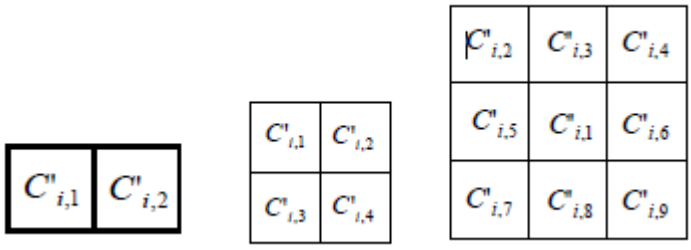



Fig.2 Different sub-blocks of the encrypted image. (a) 1×2. (b) 2×2. (c) 3×3.

the difference value in each block is computed as

$Di,j = Ci,j\,' - Ci,1\,'$ (9)

where $1 \le i \le NE$ and $2 \le j \le mE \times nE$ in Eq. (9).

As stated by the over analysis, those higher focuses of the distinction histogram need aid at present arranged In the focuses 0 What's more ±1 in the encrypted area. Likewise that in the various Awhile ago recommended DHS based RDH schemes, we could gap receptacle 0 and receptacle -1 of the distinction histogram under the inward region, and whatever remains of those bins would partitioned under those external area. Those embedding calculation of the RDH plan might a chance to be portrayed as takes after..

$Ci,j\,'' = \{\ Ci,j\,' - 1\ if\ Di,j < -1\ Ci,j\,' - b\ if\ Di,j = -1\ Ci,j\,' + b\ if\ Di,j = 0\ Ci,j\,' + 1\ if\ Di,j > 0$ (10)

In Eq. (10), $b \in \{0,1\}$ is a message bit to be embedded, and $Ci,j\,''$ is the corresponding pixel value in the marked image. Note that in Eq. (10), $2 \le j \le mE \times nE$ and $Ci,1\,'' = Ci,1\,'$. As seen, in our algorithm all pixels can be modified at most by one in the embedding process. The message extraction and image restoration can be described as follows.

$b* = \{\ 0\ if\ Ci,j\,'' - Ci,1\,'' = 0, -1\ 1\ if\ Ci,j\,'' - Ci,1\,'' = 1, -2$ (11)

$Ci,j\,'* = \{\ Ci,j\,'' - 1\ if\ Ci,j\,'' - Ci,1\,'' > 0\ Ci,j\,'' + 1\ if\ Ci,j\,'' - Ci,1\,'' < -1\ Ci,j\,''\ otherwise$ (12)

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

where $b*$ and $Ci,j'*$ represent the extracted message bit and the restored pixel value, respectively. Note that in Eq. (11) and (12), $2 \le j \le mE \times nE$ and $Ci,1'* = Ci,1''$. Following message extraction Also picture restoration, those unique encrypted picture might make recuperated by means of utilizing the concentrated area guide. If the appended bit in the location map $L$ is "1", then $Ci,j* = \{255\ if\ Ci,j'* = 254\ 0\ if\ Ci,j'* = 1$ (13)

Otherwise, $Ci,j* = Ci,j'*$ (14)

The PEHS based schemes cam wood Additionally make connected of the encrypted pictures straightforwardly in the same best approach Concerning illustration the DHS based schemes. To make this paper self-contained, three representative predictors are exemplified in Fig. 3. For all these three predictors, the values of pixel $x$ are predicted by the values of its neighboring pixels, and the predicted pixel value is represented by $\hat{x}$ .

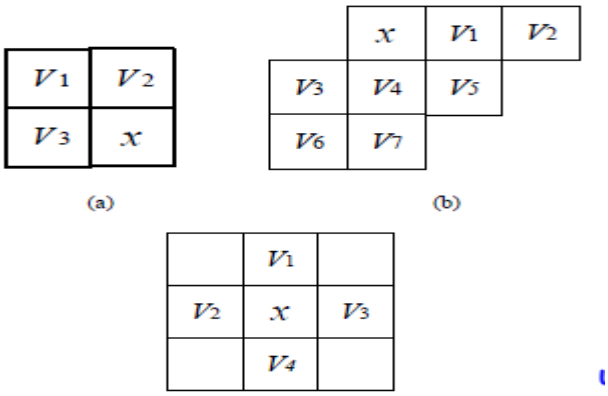



Fig.3 Three prediction algorithms.

The first one is the median edge detector (MED) [22], which is employed as context adaptive predictor in many RDH schemes [23-25]. The predictor is as follows (see Fig) $\hat{x}$ = {max($v2$, $v3$) if $v1 \le$ min($v2$, $v3$) min($v2$, $v3$) if $v1 \ge$ max($v2$, $v3$) $v2 + v3 - v1$ otherwise (15) where $v1$, $v3$ and $v3$ are the diagonal, above and left neighbors of $x$. The second one is the gradient-adjusted prediction (GAP) [26], which is employed in [27] and is more accurate than MED in if $dv - dh > 80$ $v1+u$ 2 if $dv-dh\in(32,80]$ $v1+3u$ 4 if $dv-dh\in(8,32]$ $u$ if $dv - dh \in [-8, 8)$ $v4+3u$ 4 if $dv-dh\in[-32,-8)$ $v4+x'$ 2 if $dv-dh\in[-80,32)$ $v4$ if $dv - dh < -80$ (16)

where $dv = |v1 - v5| + |v3 - v6| + |v4 - v7|$ and $dh = |v1 - v2| + |v3 - v4| + |v4 - v5|$ represent the vertical and horizontal gradients, and $u = (v1 + v4)2 + (v3 - v5)4$.

The third one is the rhombus predictor, which is employed in [10, 28]. The predicted value $\hat{x}$ is computed as follows

$\hat{x} = \lfloor v1+v2+v3+v44 \rfloor$ (17)

where $\lfloor \gamma \rfloor$ is an work that rounds the component $\gamma$ of the closest basic short of what or equivalent to $\gamma$. By means of utilizing these three predictors, the extra message odds could make inserted by means of modifying those prediction lapse histogram.

## V. CONCLUSION

In the modern digital age, the encryption process is often conducted by the transmitter, and the RDH (reversible data hiding) algorithm is often conducted by the server manager. Hence, those above-mentioned two procedure if a chance to be free for one another. In this paper, we exhibit another skeleton which permits those various RDH schemes created in front of to non-encrypted pictures make directed in the encrypted Web-domain straightforwardly. The main contributions of this paper are as follows. A new specific beck encryption algorithm is proposed to bottle some alternation amid the adjoining pixels.. Moreover, the following permutation step can completely scramble the image, and thus the information disclosure in the first step cannot be fully exploited to decrypt our encryption algorithm. On our framework, those reversible information concealing algorithm is autonomous of the picture encryption algorithm, What's more consequently hundreds for formerly recommended DHS (difference histogram shifting) and PEHS (prediction-error histogram shifting) based RDH schemes can be accomplished in encrypted domain directly and hence no need to design additional specific RDH scheme. The suggested skeleton will be suitableness to the distinct reversible data-hiding plan in encrypted image, which can offer relatively high payload and error-free data extraction.

## REFERENCS:

[1] J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5646997, 1997.

[2] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits System and Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[3] Z. Ni, Y. Shi, N. Ansari, S. Wei, "Reversible data hiding," *IEEE Trans Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[4] Y. Qiu, Z. Qian, and L. Yu, "Adaptive Reversible Data Hiding by Extending the Generalized Integer Transformation," *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 130-134, 2016.

[5] S. K. Lee, Y. H. Suh, and Y. S. Ho, "Reversible image authentication based on watermarking," in *Proc. IEEE International Conference on Multimedia and Expo (ICME)*, Toronto, Ontario, Canada, pp. 1321–1324, Jul. 9-12, 2006.

[6] X. Li, B. Yang, T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Processing*, vol. 20, no. 12, pp. 3524–3533, 2011.

[7] X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogram-shifting-based reversible data hiding," *IEEE Trans. Image Processing*, vol. 22, no. 6, pp. 2181-2191, 2013.

[8] W. Zhang, X. Hu, X. Li, N. Yu, "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," *IEEE Trans. Image Processing*, vol. 22, no. 7, pp. 2775-2785, 2013.

[9] Y. Yan, W. Cao, and S. Li, "High capacity reversible image authentication based on difference image watermarking," in *Proc. IEEE International Workshop on Image Systems and Techniques (IST)*, Shenzhen, China, May 11-12, 2009.

[10] V. Sachnev, H. J. Kim, J. Nam, S. Suresh and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 19, no.7, pp. 989–999, 2009.

**AUTHOR DETAILS:**


| | |
|---|---|
|  | **G.Swathi** pursuing M.Tech(CSE) from SREE VISVESVARAYA INSTITUTE OF TECHNOLOGY & SCIENCE, Chowdarpalle, Devarkadra(Md), Mahabubnagar(D), TS – 509204. |
|  | **Mr. A. Ranjith Kumar** is working as Assistant Professor, Department of (CSE), **SREE VISVESVARAYA INSTITUTE OF TECHNOLOGY & SCIENCE**, Chowdarpalle, Devarkadra(Md), Mahabubnagar(D), TS – 509204. |