International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 05 | May 2021 www.irjet.net p-ISSN: 2395-0072

A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms

Pallavi M O[1], Femina Auxilia F[2]

[1]*Assistant Professor, Dept. of MS in Computer Science, REVA University, Karnataka, India*
[2]*Dept. of MS in Computer Science, REVA University, Karnataka, India*

Abstract - *Reversible information covering up in scrambled pictures (RDHEI) has been presented for protecting picture security and information inserting. RDHEI typically includes three gatherings; to be specific, the picture supplier, information hider, and recipient. On the security with key setting, there are three classes: share autonomous mystery keys (SIK), shared one key (SOK) and offer no mysterious keys (SNK). In SIK, the picture supplier and information hider should separately what's more, freely share secret keys with the collector, though in SNK, no mysterious key is shared. Notwithstanding, the writing works proposed SNK-type plans by utilizing homomorphic encryption (with excessive calculation cost). In this paper, we address shared one key (SOK) setting, where just the picture supplier shares a mysterious key with the recipient, and the information hider can insert a mysterious message with no information on this key. To understand our SOK conspire in a straightforward way, we propose another method by utilizing multi-secret sharing as the hidden encryption, which surely initiates an explode issue of the key size. For safeguarding the proficiency of the key size, we apply a pressure by utilizing lightweight cryptographic calculations. At that point, we show our SOK plot dependent on the proposed methods, and show viability, productivity, and security by tests and investigation.*

Key Words: **Reversible Data Hiding, Image Privacy, Encryption, Multi-Secret Sharing, Security**

1.INTRODUCTION

Reversible information covering up (RDH) is an idea that permits to implant the extra and mystery message into cover media, like military or clinical pictures, and to play out a reversible method that separates the secret mystery message and consummately recreates the first cover content. Various reversible information concealing techniques have been presented throughout the last two many years. Two fundamental thoughts of RDH are distinction development (proposed by Tian [1]) and histogram moving (proposed by Ni et al. [2]). In the distinction extension strategy [1], the contrasts between two nearby pixels are multiplied to Y. C. Chen is with the Department of Computer Science and Engineering,

H. Hung is with the Department of Computer Science and Information Designing, National Taiwan University, Taipei, Taiwan. S. H. Hsieh is with the Institute of Information Science, Academia Sinica, Taipei, Taiwan.C. W. Shiu is with the Department of Education Industry and Digital Media, Public Taitung University, Taitung, Taiwan. Composition got ; reconsidered . discharge another most un-critical piece (LSB) plane for conveying the mysterious message. In the histogram moving strategy [2], the zero and pinnacle focuses are utilized to install the mysterious message by somewhat adjusting the pixel esteems. Numerous RDH considers have explained these two ideas to improve payload and picture quality [3, 4, 5, 6, 7, 8, 9]. As of late, another course of RDH known as RDH over an encoded picture (RDHEI) has been presented. This tale RDHEI idea was right off the bat presented by Zhang in 2011 [10], what's more, catches the accompanying genuine situation in regards to proprietor security known as picture protection [10]. A second rate aide or on the other hand a direct head is in a work process.

what's more, is approved to embed some extra information like the source data, picture documentations or confirmation information, inside the encoded picture, where the first picture content is obscure to this gathering. In fact, clinical pictures are encoded for saving the patient security, and a data set head just inserts a couple of information into the relating scrambled pictures. For the consistency of a clinical picture, it should ensure that the first substance can be entirely remade after decoding then-extraction of the mysterious message by the recipient. That is, RDHEI not just ensures the precision of the recreated cover-picture and removed mystery message which are two essential errands of RDH, yet in addition saves the the recipient R can recuperate the first cover-picture and afterward remove the mysterious message accurately. The strategy run by R is known as unscrambling then-extraction. Notwithstanding, the collector likewise can be partitioned into two stages (unscrambling and extraction). We indicate these two stages to two sorts of beneficiaries, Rdec and Rext, and Rdec performs decoding, and Rext takes Rdec's decoded picture to remove the mysterious message.

1.1 Related work

An exhaustive review on RDH is introduced by Shi etal. [11] to profoundly dissect and feature the advances of RDH for the new advancement. It considers parts of RDH, counting RDH into picture spatial area [1, 2], RDH into picture packed space (e.g., JPEG) [12, 13, 14], RDH

reasonable for picture semi-delicate verification [15, 16, 17], ... IEEE Transactions on Information Forensics and Security,Year:2019 1556-6013 (c) 2018 IEEE. Individual use is allowed, however republication/reallocation requires IEEE consent. See http://www.ieee.org/publications_standards/distributions/rights/index.html for more data.

This article has been acknowledged for distribution in a future issue of this diary, however has not been completely altered. Substance may change before conclusive distribution. Reference data: DOI 10.1109/TIFS.2019.2914557, IEEE Exchanges on Information Forensics and Security and so forth Specifically, it likewise examines RDHEI, and orders the current RDHEI plans into two classes: abandoning room prior to encryption and emptying room after encryption by inserting methodologies. For key setting, Shi et al. [11] too referenced the other idea, purported RDHEI dependent on open key encryption. In any case, roused by the factor of key setting, the present considers recognize the accompanying two thoughts of RDHEI.

- **Share autonomous mystery keys (SIK)** R shares free keys, keyP and keyH, with P and H separately. Prominently, these keys (keyP , keyH) are secret and used to run picture encryption and implanting calculations. Various keen works [10, 18, 19, 20, 21, 22] have proposed this sort of RDHEI plans.

- **Share no mysterious key (SNK)** Rather than SIK, R does not have to share any mysterious key. This can be without any problem accomplished through open key encryption where R has a public/secret key pair, and P (H, resp.) can utilize the general population key to do picture encryption (information inserting, resp.).The first arrangement, proposed by Chen et al. [23], is to utilize Paillier homomorphic encryption [24] to encode each pixel and depend on explicit procedures to finish information inserting. With the utilization of the homomorphic encryption, the subsequent works of Zhang at al. [25], Li and Li [26], and Shiu et al. [27] individually carry out a few reversible information concealing methods under the public key encryption related with the homomorphic property. To sum up the adaptability of key setting, unmistakably just the assigned party who has the mysterious key can be P or then again H in SIK. In any case, the upside of SNK is that anybody can be P or H, since the keys of encryption or inserting are actually the public key. Moreover, as known, those homomorphic encryption-based SNK-type RDHEI plans are basically wasteful since the fundamental encryption plans generally depend on muddled variable based math structures and spend high computational expense. It does the trick to give the accompanying inquiry, also, we will target tending to it in the rest of this paper. Would we be able to build a productive plan to fulfill the transitional idea (among SIK and SNK) where P and R share a mysterious key, yet no mystery is shared with H? Truth be told, Wu et al. [28] had proposed a common one key (SOK) conspire dependent on secret sharing. Notwithstanding, their strategy spends much space cost, since it encodes a pixel into n shares, where n is the security boundary of mystery sharing, and the absolute expense of a scrambled pixel will explode to 8n pieces.

1.2 Primary Contributions

Allow us momentarily to sum up our outcomes. Our beginning stage is to formalize the new idea of key setting and care about 1The key setting offers the structure among P, H, and R. For instance, in the event that a RDHEI conspire is under open key encryption, any one can be P and H. On the off chance that under a symmetric encryption among P and R (H and R, resp.), as it were explicit gathering who holds the common mystery key can be P (H, resp.). The key use is alluded to as gathering adaptability. In the accompanying, we formalize the key setting for additional subtleties. the proficiency. To accomplish better proficiency, we should keep away from utilizing public key encryption. Nonetheless, in the event that we don't utilize any public key encryption conspire, it is difficult to secure picture security (the first motivations behind RDHEI) without the common key among P and R. Along these lines, for safeguarding protection, the ideal class is that beneficiary offers "just one" secret key with the picture supplier (SOK, for short). Specifically, there is no divided key among H and R, which correctly suggests that the implanting method doesn't accept any common key as info. The proposed SOK plans are propelled from some current SNK plans (i.e., [25, 27]). We tracked down that these SNK plans work with Paillier encryption (or other expansion homomorphic encryption) to safeguard picture security, and the property of homomorphic assessment is utilized to insert the message. For accomplishing our previously mentioned necessities, we supplant the pieces of Paillier encryption with secret sharing that additionally appreciates homomorphic assessment in some ways2 . We show a deliberation of those SNK plans, and afterward under the reflection, present our technique. The general thought of our technique is made out of the accompanying two stages.

- **Encryption.** Secret sharing goes about as a symmetric encryption to encode the cover-picture, so our technique utilize one divided key among P and R. Notwithstanding, our own doesn't develop shares for every pixel like Wu et al's. strategy. For protecting the complete size, we pack t pixels and t arbitrary factors together to produce just t offers, and put the offers back as scrambled pixels and set arbitrary components as the key. It does the trick to keep away from the size explode, and furthermore keeps accuracy of unscrambling by utilizing t irregular components furthermore, t shares. The procedure of our technique is motivated by the multi-secret

sharing, yet we marginally adjust it for security and structure of SOK.

- **Data implanting**. We partition the mysterious message into a few units. At that point, for inserting a unit, we create another t shares without requiring any key (as known as the previously mentioned irregular components), and afterward use homomorphic assessment and inserting strategy to insert message into the t scrambled pixels.

The proposed strategy stringently depends on the properties of mystery sharing. Summing up the primary methods, secret sharing fills in as the fundamental crude contribution security, various mystery jam size intricacy, and intrinsically added substance homomorphism understands the information installing. We give the formal portrayal of the procedure, and present a reasonable idea, alleged working expansion homomorphism in multi-secret sharing (OAMSS). Furthermore, we likewise give another strategy to pack the size of a key utilized in OAMSS. For speculation, if SNK plans fulfill a few properties, they can be changed over to SOK. Consequently, our strategy can be summed up as a converter. As a solid launch, given Shiu et al's. SNK plot dependent on contrast extension, we show the SOK-type RDHEI by slight change. The plot outline is portrayed as follows. P will pre-measure the cover-picture (counting twofold the contrasts between two)

1.3 Organization

The rest of this paper is organized as follows. In Section II, we will introduce some preliminaries, including secret sharing and polynomial interpolation, and a clean abstraction of the existing SNK-type RDHEI schemes. Then, in Section III, our techniques are formally presented. A demonstration (associated with its experiments and discussions) will presented in Section IV. Finally, our conclusions of this paper are given in Section VI. In Appendix, we provide some missing details. We will review Paillier additive homomorphic encryption which is used to construct SNK-type schemes. Then, we will show how to handle side information in our scheme. Given the SNK-type scheme of Zhang et al. [25], we demonstrate an alternative SOK-type scheme. Finally, we state our converter and show how to convert SNK with specific properties to SOK.

2 . Primers

2.1 Secret Sharing

The thought of k-out-of-n edge secret sharing was first presented by Shamir [29], where a genuine vendor takes a secret as info, and produces n shares for n parties (each gathering 3 Indeed, the pre-handling additionally manages area map which is utilized to record the unembeddable pixel sets. gets one offer), to such an extent that any k offers (k < n) can recuperate the first mystery. In the writing, secret sharing was most certainly not just a cryptographic plan, yet in addition goes about as a principal building block for tackling a lot of examination issues and issues. Foundation information. Shamir secret sharing plan is in light of polynomials over a limited field F, where |F| > n is stringently required. In view of some known hypotheses, any k sets (xi , yi) ∈ F × F with particular {xi} can interestingly decide a polynomial f of degree (k − 1) to such an extent that f(xi) = yi for I ∈ [1, k], where I ∈ [zlow, zupper] indicates zlow ≤ I ≤ zupper, also, I, zlow, and zupper are numbers. To build the polynomial f, one can utilize the Lagrange Insertion over a limited field F 4 . For I = 1, ..., k, a degree-(k − 1) polynomial is characterized as followsδi(X) ≡ Qk j=1,j6=i(X − xj) Qk j=1,j6=i (xi − xj) to such an extent that δi(X) fulfills δi(xi) = 0 for I 6= j 1 for I = j Set f(X) ≡ Pk i=1 δi(X) · yi. In this way, f is the remarkable degree-(k − 1) polynomial fulfilling f(xi) = yi for all I ∈ [1, k]. Development of Shamir (k, n)-edge secret sharing conspire. Leave F alone the limited field fulfilling S ∈ F and |F| > n.Let x1, .., xn ∈ F be particular, nonzero components that are fixed also, freely known.

- **Sharing:** Given a mysterious S ∈ F, the seller picks uniform a1, ..., at−1 ∈ F and characterizes the polynomial f(X) = S + Pt−1 i=1 aiXi , where S is the steady term in f. A gathering Pi gets an offer (xi , yi), where yi = f(xi) ∈ F and xi signifies Pi's character.

- **Reconstruction:** To recuperate the mystery, k gatherings report their offers. On the off chance that the k gatherings gather their k shares together, it gets the job done to recuperate the polynomial f by Gaussian end and get the mysterious S = f(0).

For security, Shamir secret sharing plan ensures that any not exactly k offers can't recuperate S, and hence no data about S can be uncover. It is likewise unequivocally secure, where benefit of the unbounded force assailant is indistinguishable to irregular speculating as known as genuine security. In this paper we overlook conversation of the all around examined thought, secret sharing. All things being equal, we portray an all the more remarkable usefulness called multi-secret sharing offered by Shamir secret sharing. By and large, in the k-out-of-n edge case, the seller takes d mysteries, S1, ..., Sd, to deliver n shares, and any k offers work together to recuperate every one of these mysteries. In any case, assume there is an enemy who can ruin c offers (c < k). For this situation, in the event that the foe has no data about S1, ..., Sd, we say this mysterious sharing plan is a (c, d, k, n)- multi-secret sharing 4For improving on the show, we will exclude to show mod F in equal

Theorem 1 (Bound of multi-secret sharing [30], informal). There exists a (k − d, d, k, n)-multi-secret sharing scheme to share d secrets among n parties, d ≤ k < n. In this paper, we start with the multi-secret sharing scheme. We put d secrets in some coefficients of polynomial f, and keep using uniform randomness in the other coefficient. According to the bound, the system

parameters are set as d = t, k = 2t and n = 2t, which suffices to offer unconditional security guarantee.

B. Systems of SNK and SOK-type RDHEI A SNK-type RDHEI technique includes three gatherings (picture supplier P, information hider H, and recipient R) and comprises of the three algorithms6 as follows.

• Image-Encryption: this calculation, run by P, takes a cover-picture and the beneficiary's public key as contribution to create the encoded picture.

• Message-Embedding: this calculation, run by H, takes an scrambled picture, an objective message and the collector's public key as contribution to insert the message.

• Decryption-then-Extraction: this calculation, run by R, takes an encoded picture with installed message and the beneficiary's mysterious key as contribution to get the stego-picture by decoding, and afterward separate the message and recuperate the cover-picture from the stego-picture. For regent precision, we necessitate that the reproduced cover-picture and message in the phase of Decryption-thenExtraction should be indistinguishable from the first cover-picture encoded in Image-Encryption and the message covered up in Message-Embedding. In the following segment, we give an reflection of existing SNK-type RDHEI plans dependent on Paillier encryption. In any case, SOK-type RDHEI plans are somewhat extraordinary from SNK. The properties of SOK are that P and R shares a mysterious key which is simply used to encode the picture and unscramble, and they don't have any common mystery with H. This suggests that any gathering can go about as the information hider in SOK.

Comment 1. In SOK, P and R introduce a common key. This setting follows the situation of mystery key encryption. They share the key with a safe channel at the framework arrangement. In any case, to convey an offer key with no safe channel, a straightforward way is to utilize commonplace public key encryption. C. Reasonable Abstraction of the Existing SNK-Type RDHEI Plans dependent on Paillier Encryption Some current SNK-type RDHEI plans depend on Paillier Encryption. The Paillier encryption is a public key encryption that empowers added substance homomorphic activity such that Enc(m1) NEnc(m2) = Enc(m1 + m2), where N is 5 In the event that the aggressor could acquire some direct imperatives among S1, ..., Sd, some data about the insider facts would be uncovered and it would disregard unlimited security. 6We exclude a few subtleties of calculations. Here, just present the undeniable level. precisely augmentation. More subtleties of Paillier encryption are momentarily summed up in Appendix A. The primary thoughts of those current SNK-type RDHEI plans [25, 27] are momentarily portrayed as follows.

•Image-Encryption: plays out some pre-handling for the entire cover-picture, and afterward utilizes the Encrypt calculation of Paillier to encode every pixel pi and produce the encoded picture EncR(pi).

•Message-Embedding: plays out some pre-handling for the message that H needs to implant, and afterward employments Scramble to encode the handled outcome for each unit si , and afterward creates the scrambled form EncR(si). At long last, this calculation yields EncR(p 0 I) = EncR(pi) NEncR(si) as the encoded picture with an implanted message.

•Decryption-then-Extraction: runs Decrypt to recuperate p 0 I , and afterward removes the mysterious string and acquires the coverimage.We don't guarantee that a particular pre-preparing is utilized, since various plans, for example, [27] and [25] receive diverse preprocessing methods. Here, we just need to guarantee that the message installing is finished by added substance homomorphic assessment. The above theoretical deliberation decouples th usefulness of information covering up (counting pre-preparing and extraction) and the security of picture protection. In Section IV, we will show an exhibit dependent on the plan of Shiu et al. [27], and additionaly give an option dependent on Zhang et al. [25] in Appendix.

3. Strategies from Light weight cryptographic

Calculations In this part, we will depict our strategies from lightweight cryptographic calculations. In Section III-A, we present another strategy to work expansion homomorphism in multi-secret sharing. In Section III-B, to deliver a critical enormous size of arbitrariness, we give a compacting procedure by utilizing lightweight cryptographic natives.

3.1 Strategy I

Operating expansion homomorphism in multisecret sharing (OAMSS) This strategy OAMSS is three-overlap. We casually feature the structure and afterward depict the subtleties.

- **OAMSS.Set**: It gives a multi-secret sharing-based way to deliver the mysterious key (meant by R) furthermore, scramble t information together. The plain information are meant by p1, ..., pt, and the encoded ones by EncR(p1), ..., EncR(p1).
- **OAMSS.Add:** Without any data of the key, it works expansion homomorphism in these t scrambled information; for instance, adding si in EncR(pi),. It at last can get EncR(p1 + s1), ..., EncR(pt + st).
- **OAMSS.Recover:** By performing unscrambling with the key R, it can have p 0 I like p 0 I = pi + si for every I. Allow us to expand the specialized subtleties for understanding these three calculation by utilizing multi-secret sharing.

- **OAMSS.Set:** Initially, we produce a mysterious key R = (rt, ..., r1) by haphazardly choosing ri from F for every I. Given IEEE Transactions on Information Forensics and Security,Year:2019 1556-6013 (c) 2018 IEEE. Individual use is allowed, yet republication/reallocation requires IEEE consent.

This article has been acknowledged for distribution in a future issue of this diary, yet has not been completely altered. Substance may change before definite distribution. Reference data: DOI 10.1109/TIFS.2019.2914557, IEEE Exchanges on Information Forensics and Security 5 an objective information rundown of t components over a field F, signified by P = (pt, ..., p1) and pi ∈ F, this does the trick to deliver a polynomial f (modulo F) by putting the components of R and P on the coefficients, for example, f(x) = ptx 2t−1 + ... + p1x t + rtx t−1 + ... + r1x 0 (modF). Utilizing the public personalities ID1, ..., IDt as focuses, f(ID1), ..., f(IDt) are delivered as the scrambled information. Set (EncR(p1), ..., EncR(pt)) as (f(ID1), ..., f(IDt)). OAMSS.Add: Given st, ..., s1, this likewise does the trick to create a polynomial f 0(modulo F) by putting them on the primary t coefficients, for example,g(x) = stx 2t−1 + ... + s1x t (modF). As the abovementioned, we acquire g(ID1), ..., g(IDt), and afterward process f 0 (IDi) = f(IDi) + g(IDi) for every I. At long last, set (EncR(p 0 1), ..., EncR(p 0 t)) as (f 0(ID1), ..., f0 (IDt)). OAMSS.Recover: We straightforwardly acquire t conditions where f 0 (IDi) = p 0 T (IDi)2t−1 + ... + p 0 1(IDi) t + rt(IDi)t−1 + ... + r1(IDi) 0 for all I, 1 ≤ I ≤ t. Note that f 0 (IDi), IDi , rt, ..., r1 are known, so this suggests that p 0 t , ..., p0 1 are extraordinarily characterized by Gaussian end. Subsequently, we can recuperate p 0 t , ..., p0 1such that p 0 I = pi + si. For accuracy, we should guarantee that OAMSS.Recover can recuperate the right worth of p 0 I fulfilling p 0 I = si + pi . For security, we use (t, t, 2t, 2t)-multi-secret sharing to ensure the security of the encoded information.

3.1.1 Correctness:

Initially, OAMSS.Set and OAMSS.Recover have a common key (r1, .., rt). To produce f, OAMSS.Set sets the key and information as the coefficients of the polynomial f(x) = ptx 2t−1+...+p1x t+rtx t−1+...+r1. At that point, it makes t shares {EncR(pi)} t i=1 which are upsides of f(x), by taking care of each {IDi}t i=1 in x. After getting {EncR(pi)} T i=1, OAMSS.Add will utilize s1, ..., st to supply coefficients of the polynomial g(x) = stx 2t−1 + ... + s1x t, and afterward makes {EncR(si)} T i=1 with the previously mentioned taking care of way in x, and adds it to {EncR(pi)}t i=1 to acquire {EncR(p 0 I)} t i=1. The such preparing obviously holds EncR(p 0 I) =f(IDi) + g(IDi) =(p 0 t)(IDi)2t−1 + ... + (p 0 1)(IDi) t + rt(IDi) t−1 + ... + r1, where p 0 I = pi + si for I ∈ [1, t]. At long last, OAMSS.Recover gets {EncR(p 0 I)} t i=1. It accepts the obscure p 0 j for every j ∈ [1, t] and makes the polynomial f 0 (x) = (p 0 t)(x) 2t−1 + ... + (p 0 1)(x) t + rt(x) t−1 + ... + r1,where r1, ..., rt are known for OAMSS.Recover. At that point, it produces t conditions by subbing {IDi}t i=1 into f 0 (x) and the upsides of {EncR(p 0)}t i=1. Since the particular {IDi} t i=1 are known, by utilizing Gaussian disposal over t conditions as Figure 1,

p 0 1 , ..., p0 t can be accurately recuperated.

EncR(p 0 1) = (p 0 t)(ID1) 2t−1 + ... + (p 0 1)(ID1) t + rt(ID1) t−1 + ... + r1

EncR(p 0 2) = (p 0 t)(ID2) 2t−1 + ... + (p 0 1)(ID2) t + rt(ID2) t−1 + ... + r1

EncR(p 0 t) = (p 0 t)(IDt) 2t−1 + ... + (p 0 1)(IDt) t + rt(IDt) t−1 + ... + r1

Fig. 1: t conditions, where the p 0 I is obscure

3.1.2 Security:

The motivation behind security is to ensure the contain of the first information. Accept that the assailant is semihonest and can listen in just on scrambled information. We utilize the (t, t, 2t, 2t)- multi-secret sharing, and our plan uncovers as it were the t-shares as scrambled information. In this manner, Theorem 1 assurances that the plain information is secured. Also, the mysterious sharing requires the limit should not exactly the measured, and along these lines we need to painstakingly set 2t < F for keeping accuracy.

3.2 Strategy II

Compression for irregularity creation To finish Technique I, we need to create a huge huge size of irregularity as the key (i.e., t arbitrary components). The objective of Technique II is to utilize the short contribution to produce a long irregular yield. We apply a standard strategy to figure it out key size pressure given a pseudorandom work (PRF) F : {0, 1} n × {0, 1} n → {0, 1} (n is the framework boundary). The such PRF takes a n-bit arbitrary key and n-bit input, and at that point returns a n-digit yield. With the supporting by PRF, we just need to set up a n-bit key indiscriminately (indicated

4. Demonstration: SOK-TYPE RDHEI FROM DIFFERENCE EXPANSION

In this section, we describe a set-up for image pixels based on the difference expansion method. Then, we show a full demonstration of the SOK-type RDHEI scheme by using Technique I. We do not discuss or analyze correctness and security for the following scheme, since the details can be referred to Section III-A.

4.1 Set-up

According to the system overview in Section I-B, the kernel hiding method is based on the difference expansion technique and the protection is achieved by secret sharing.

Following the notion of difference expansion, we denote a pixel pair by (x, y), and compute l = b x+y 2 c, d = x − y, x 0 = l + d and y 0 = l − d. Here, we define (x 0 , y0) as the new pixel pair for embedding the secret message. Moreover, to preserve the security of secret sharing, the size of the field F must be a prime number, and thus we choose 251 as the size of F which can be encoded to 8-bit. In the following, the size of field F is 251. Before describing the details of the proposed method, we must rule out some cases of pixel pairs by defining the following pixel pairs categories.

• Unembeddable (constrained by difference expansion): If any one of x 0 and y 0 is more than 255 or less than 0, we say this pair is unembeddable.

• Non-embedded (constrained by secret sharing): The range of a pixel is from 0 to 255. We set the size of F as 251, which implies we must discard five types of pixel values before image encryption for pixel pair (x 0 , y0). Let P be a set of pixel values to be encrypted via secret sharing such that |P| = 251. Let P¯ be a mutually exclusive set of P, with size |P¯| = 5. If a pixel pair (x 0 , y0) is not unembeddable but any one of its two pixel values is in P¯, we say this pair is non-embedded.7

• Nice: A pixel pair that is not unembeddable and also not non-embedded is defined as a nice pair. Note that a meaningful image is usually a smooth image, and thus the values of pixel pairs are not usually unembeddable. When using secret sharing to encrypt pixel pairs, we could choose the five lowest frequent pixel values to be P¯. However, sending unembeddable and non-embedded pixel pairs is not complicated. We can send them as side information. The missing details to deal with side information are in Appendix B. In the following subsection, we consider that the pixel pairs are nice in performing encryption and message embedding.

5. Concrete Method

We describe our scheme by using t/2 pixel pairs as a pack and OAMSS. The difference expansion method in the scheme is similar to that in [1] and identical to that of [27]. Figure 2 illustrates the sketch of the proposed method (associated with 7There are some standard techniques to transform [0, 255] to [0, 250] with small overhead for side information [1]. an example). Construction. We distribute a set of t pixels, and obtain t/2 pixel pairs (xi , yi) for i ∈ [1, t]. For each i ∈ [1, t], we generate distinct and public IDi ∈ F, and then performs following steps. • Key generation: This algorithm randomly chooses a key and uses Technique II to obtain {r1, ..., rt}, where r1, ..., rt ∈ F. • Image-Encryption: This algorithm individually preprocesses each pair (xi , yi) to compute `i = b xi+yi 2 c and di = xi − yi , and then computes x 0 i = `i + di and y 0 i = `i − di . We remark that di can be positive or negative. It sets (p1, ..., pt) = (x 0 1 , y0 1 , ..., x0 t/2 , y0 t/2) for i ∈ [1, t], and then, with {ri} t i=1, works as following steps. 1. It generates a polynomial f(x) = ptx 2t−1 + ... + p1x t + rtx t−1 + ... + r1 such that f : F 7→ F. 2. It obtains {(IDi , yi)} t i=1 such that yi = f(IDi). Finally, the algorithm sets the encrypted version of a pixel EncR(pi) = yi . • Message-Embedding: For the secret message m = (m1, ..., mt/2), this algorithm generates an expansion as s = (m1, 0, m2, 0, ..., mt/2, 0). It then parses s as (s1, ..., st). Subsequently, with the pairs {IDi , EncR(pi)} t i=1, the algorithm works with the following steps. 1. For each i ∈ [1, t], it computes y s i = st(IDi) 2t−1 + ... + s1(IDi) t . 2. It sets EncR(si) = y s i and outputs EncR(spi) = EncR(si) + EncR(pi) as the encrypted version with the embedded message. Note that the bit of secret message is only put in the first position in a pixel pair. • Decryption-then-Extraction: This algorithm works, with key {ri} t i=1, as follows. 1. It sets unknown sp0 i ∈ F × F for i ∈ [1, t]. 2. It generates a polynomial f 0 (x) = sp0 tx 2t−1 + ... + sp0 1x t + rtx t−1 + ... + r1. 3. By substituting the pairs {IDi, EncR(spi)} t i=1, it obtains t equations: EncR(spi) = sp0 t (IDi) 2t−1 + ... + sp0 1 (IDi) t + rt(IDi) t−1 + ... + r1. 4. By Gaussian elimination, it obtains sp0 i for i ∈ [1, t] from solving the t equations. Finally, with the stego-image, the algorithm extracts the secret message with the procedure: parsing {sp0 i } t i=1 as t/2 pairs denoted by (x 00 j , y00 j) for j ∈ [1, t 2]. If x 00 and y 00 are both odd or both even, R extracts mi = 0 and recover x 0 i = x 00 i and y 0 i = y 00 i ; if not, R extracts mi = 1 and recovers x 0 i = x 00 i − 1 and y 0 i = y 00 i since mi is embedded only in the first pixel. R can easily compute `i = b x 0 i+y 0 i 2 c and di = x 0 i−y 0 i 2 and easily obtain the original pixel pair in the cover-image by computing xi = `i + b di+1 2 c and yi = li − b di 2 c. It completes the cover-image recovery. Example 2. This example is in Figure 2. Suppose a pair of pixels with pixel values, (102, 100). Using the preprocessing.

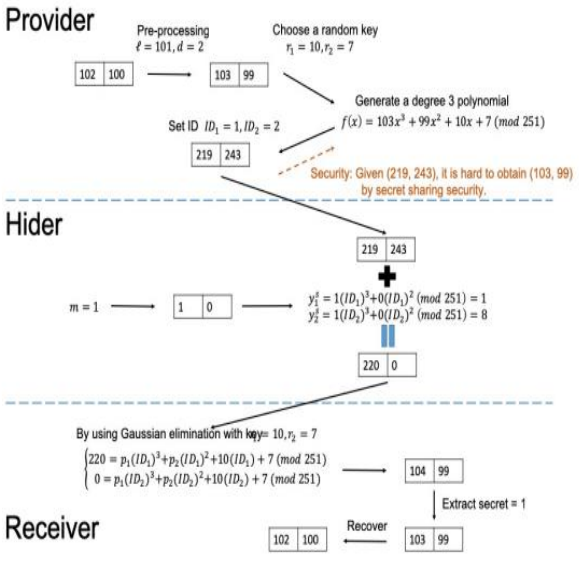

Fig.2 : The sketch of the proposed SOK-type method(take t=2 and a fixed pixel pair as an example)

6. COMPARISONS

6.1 Security and Experiments

Remark 2. We recap a fact of stream-cipher-based SIK schemes with respect to security [31]. This work points

out the weakness of stream-cipher-based SIK schemes, i.e., [10, 19, 21, 22]. However, such the attack does not appear in (multi-) secret sharing and Paillier-based schemes. The testing images and encrypted results shown in Figure 3 are of the proposed scheme. There is no information leakage on the encrypted images. With the security advantage, we further discuss the effectiveness in the aspects of payload and image quality. We focus on the results of proposed scheme, presented in Section IV, at first, and postpone the comparisons with IEEE Transactions on Information Forensics and Security,Year:2019 1556-6013 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2019.2914557, IEEE Transactions on Information Forensics and Security 8 TABLE I: The maximum payload Scheme Payload (bpp) [10] 0.003 [19] 0.004 [21] 0.031 [22] 0.038 [33] 0.072 [27] 0.498 [25] 0.423 [32] 0.384 Our scheme 0.498 the relevant schemes to the next paragraph. For payload and image quality, experiments are shown in Figure 4 by taking a few typical cover-images. According to the results shown in Figure 4, we conclude that the proposed SOK-type method inherits the properties from the use of difference expansion (DE), and thus it leads better PSNR and payload in smooth images (like Lena). In addition, we compare our scheme with some typical and state-of-the-art works [10, 19, 21, 22, 25, 27, 28, 32, 33] on Lena and Baboon which are representatives of smooth and complex images. The comparison results are provided in Figures 5 and 6 respectively. However, difference expansion like schemes (including [27, 28] and the proposed) enjoy almost identical PSNR and payload, and the extremely negligible difference comes from the use of underlying encryption. Finally, in Appendix C, we will show an alternative solution by modifying from the scheme of Zhang et al. [25]. Its payload and PSNR are almost identical to the results of [25] as well. Finally, we use 10 random images from the USC-SIPI image database and perform the experiments for the maximum payload. The results are shown in Table I. The schemes of [10, 19, 21] are based on LSB flipping, and thus payload is bounded. However, to increase payload is achieved by shrinking the size of blocks, but this cannot recover the coverimages. As a result, only less payload can guarantee lossless image recovery in these schemes [10, 19, 21]. The scheme of [22] use pre-processing to restrict the number of peaks in the encrypted image, but preserve nice image quality. That of [23] applies the traditional RDH method, and also preserve nice payload and image quality. However, that of [27] relies on pre-processing for different expansion, except for some cost of the location map, payload is close to 0.5bpp. That of [25] also can achieve 0.5bpp ideally (the results are influenced by the setting of threshold). Finally, the scheme of [32] takes the reserving room technique, where P has to perform self embedding on bit steam of target areas. However, this induces a few embedding issues, so the result is roughly 0.4bpp. Our scheme is based on pre-processing identical to [27], and thus achieve identical payload. B. Efficiency For the discussion of efficiency, we aim for two aspects, theoretical and practical results, to analyze the schemes. 1) Theoretical results: We show the theoretical analysis in Table II with asymptotic notions, where the number of pixels is denoted by N. Let p and p 0 be the size of an encrypted unit and encryption run-time of a unit in Paillier encryption.

6.2 Efficiency

For the discussion of efficiency, we aim for two aspects, theoretical and practical results, to analyze the schemes. 1) Theoretical results: We show the theoretical analysis in Table II with asymptotic notions, where the number of pixels is denoted by N. Let p and p 0 be the size of an encrypted unit and encryption un-ti me of a unit in Paillier encryption.

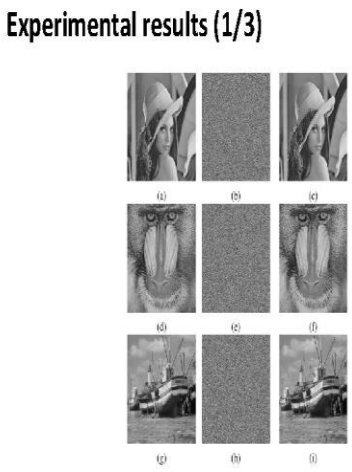

Fig. 3 : Left Cover-image.Middle:Encrypted, Right Stego(after decryption)

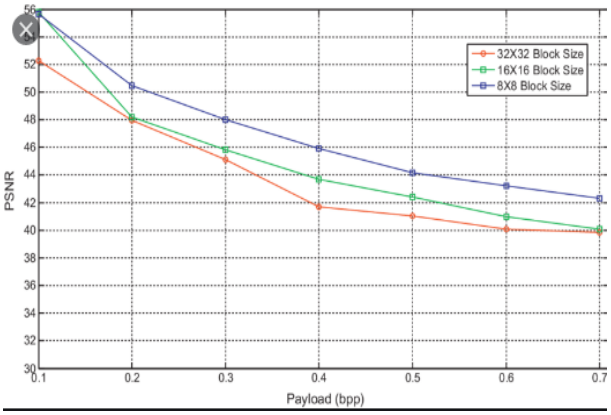

Fig. 4: PSNR and payload of the proposed SOK-type method

7. Conclusion

In this paper, we present another class of reversible information stowing away in encoded pictures, alluded to as shared-one-key (SOK). In this class, just the picture supplier has a common secret key with the beneficiary, and specifically, any individual who knows the installing system can cover up. For adaptability, SOK is a lot more fragile than SNK. Nonetheless, the current SNK plans depend on added substance homomorphic encryption. We use secret sharing as the hidden fixing to develop our SOK plan to accomplish better proficiency and safeguard the aggregate size. At that point, we convert a SNK conspire for certain properties to a SOK form. To show the viability, we give a full portrayal of the SOK plot from the SNK plans. At last, we plan to lead a resulting study, so propose a conventional converter from a SIK plan to SOK.

REFERENCES

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, pp. 890–896, 2003.

[2] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on circuits and systems for video technology, vol. 16, no. 3, pp. 354–362, 2006.

[3] W. Hong, "Adaptive reversible data hiding method based on error energy control and histogram shifting," Optics Communications, vol. 285, no. 2, pp. 101–108, 2012.

[4] S.-W. Jung, S.-J. Ko et al., "A new histogram modification based reversible data hiding algorithm considering the human visual system," IEEE Signal Processing Letters, vol. 18, no. 2, pp. 95–98, 2011.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 223–238.

[6] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," Signal Processing: Image Communication, vol. 39, pp. 226–233, 2015.

[7] X. Wu, J. Weng, and W. Yan, "Adopting secret sharing for reversible data hiding in encrypted images," Signal Processing, vol. 143, pp. 269 – 281, 2018.

[8] F. Khelifi, "On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain," Signal Processing, vol. 143, pp. 336–345, 2018.

BIOGRAPHIES

Pallavi M O, Assistant Professor, Department of Computer Science. Having 8 years of teaching experience. Research Areas: Data Mining and Networking.

Femina Auxilia F, MS in CS Student in REVA UNIVEERSITY. Area of Interest: Internet Of Things(IOT),Data Mining.