Weaknesses in Security Considerations related to Chaos-based Image Encryption

Thomas Hütter[1], Mario Preishuber[1], Jutta Hämmerle-Uhl[1], and Andreas Uhl[1]

Visual Computing and Security Lab (VISEL)
Department of Computer Sciences, University of Salzburg, Austria
andreas.uhl@sbg.ac.at

Abstract. Over the past years an enormous variety of different chaos-based image and video encryption algorithms have been proposed and published. While any algorithm published undergoes some more or less strict experimental security analysis, many of those schemes are being broken in subsequent publications. In this work it is shown that three issues wrt. chaos-based encryption security considerations severely question the soundness of these techniques. It is experimentally demonstrated that obviously weak (i.e. insecure) encryption schemes do not consistently fail commonly used tests to assess chaos-based encryption security and thus, passing these test is only a necessary condition for a secure scheme, but by no means a sufficient one. Security analysis of chaos-based encryption schemes needs to be entirely reconsidered.

1 Introduction

In the mid 1990's scientists around the world started research in the field of chaos-based image encryption, inspired by the work of Scharinger and Pichler [20] who applied the Baker map [6] to the discrete case of 2D image encryption and by the work of Fridrich [9] who extended the discretised map to 3D and composed it with a diffusion mechanism. Since then, new chaos-based image and video encryption schemes have been proposed at an almost weekly basis and a large number of corresponding publications is observed in many conferences and journals (see Table 1 for example), and the flood does not seem to be about to stop.

We concentrate on chaos-based encryption techniques applying discretised 2D chaotic maps iteratively to image matrices directly (which are also considered experimentally, i.e. [20, 9]) and do not cover techniques which XOR the visual data with pseudo-random sequences generated by chaos-based random number generators (e.g. [32]).

In this work, we will look into three security-related weaknesses of chaos-based image and video encryption schemes as follows.

1st Weakness: Security-related Motivation – a major motivation often stated for chaos-based image and video encryption is a security concern when applying cryptographically secure ciphers to images with their intrinsic features in particular "high redundancy and strong correlations among adjacent pixels" [26]. In order to justify this concern, it is common in chaos-based image and

video encryption literature to refer to the Handbook of Applied Cryptography [17]. Indeed, this resource contains several analyses which apply to encrypting redundant data. First, with respect to practical security concerns, it is stated that redundant plaintext data causes problems for synchronous stream ciphers and block ciphers with small block size, which are prone to dictionary attacks in case of using non-chaining modes like ECB. Obviously, this does not pose a security problem when applying AES in CFB mode to visual data for example. Second, with respect to a more theoretical security concern, there is a close interconnection between the redundancy of plaintext data and the unicity distance, a fact which suggests plaintext data to be as random as possible (which is not the case for classical visual data like image and video data of course). However, todays state-of-the-art encryption schemes are expected to be secure regardless of the data being encrypted. Indeed, the minimum level of security typically expected is ciphertext indistinguishability under a chosen-plaintext attack (IND-CPA). This requires that, even if an adversary may choose the messages being encrypted, (s)he still cannot distinguish the encrypted output from a random bitstring (of equal length). Currently, no attacks have been published that would violate the IND-CPA assumption wrt. AES for example. If an encryption system is severely broken, eventually the nature of the data being encrypted might affect the ability of an attacker to exploit the system's weakness. In that case, any system for which that is the case would be regarded as hopelessly insecure and unsuitable for use today. Therefore, the motivation to use chaos-based encryption for visual data instead of encryption with a cryptographically strong cipher for security reasons cannot be justified.

2nd Weakness: Many broken Algorithms – an extensive analysis of security problems in chaos-based encryption schemes in general, including an analysis of problems with selecting specific chaotic maps is given in [5] and [24] lists several principles of cryptoanalysing chaos-based encryption. A recent review on chaos-based image encryption [18] contains a good selection of papers demonstrating successful cryptanalysis of published chaos-based image encryption schemes and also [33] provides a corresponding survey-like section on successful cryptanalyses. Some examples for the classical "crypto game" in chaos-based image and video encryption, i.e. proposing techniques, which are subsequently broken and enhanced in further work (among them proposals in top quality journals, e.g. [19, 31]) are given in Table 1.

Table 1. Examples for the crypto game in chaos-based image encryption.

proposed technique ...	[3]	[3]	[7]	[12]	[31]	[25]	[29]	[10]	[19]	[11]	[27]	[9]	[9]
broken / improved by ...	[4]	[15]	[14]	[22]	[33]	[2]	[1]	[13]	[13]	[8]	[30]	[16]	[23]

Regarding the two chaos-based schemes considered experimentally also the highly referenced paper by Fridrich [9] was subject to cryptanalysis. The paper proposes an encryption scheme which is based on chaotic confusion and pixel diffusion in several iterations. Analysis of this algorithm has been done by [16] and [23]. They conduct a brute force attack, known- and selected plaintext attacks, as well as chosen-ciphertext attacks showing security problems in the algorithm.

Of course, the large amount of broken chaos-based encryption schemes gives rise to the question if current security assessment as done by the proposing authors is indeed sound (and of course, it is not in most cases as we will demonstrate).

3rd Weakness: Insufficient Security Analysis Methodology – the third security-related weakness, intrinsically linked with the second one, is a lack of systematic and sound methodology for security analysis. Of course, a weak security analysis will automatically lead to many algorithms being broken (see second weakness). While any chaos-based encryption algorithm published undergoes some more or less strict experimental security analysis, suggesting its high security standard, many of those schemes are being broken in subsequent publications (see previous subsection). The security analysis conducted in most corresponding publications usually consists of a set of (statistical) measurements applied to encrypted visual data, e.g. computing characteristics like correlation property, sequence tests, entropy or color value distribution. Other methods like NPCR and UACI [28] are used to show the resistance against differential or linear attacks like chosen-plaintext or known-plaintext attacks. Furthermore, NPCR is also used to show key sensitivity of an encryption algorithm. The first problem with this approach is that in many papers, only a limited set of images is used to derive the results and often, only some graphics are shown to qualitatively "prove" a specific property based on an example (e.g. histograms or correlation plots). The second problem, even more severe, is that even if properly conducted on sufficient data and underpinned with quantitative results, passing these tests is only a necessary condition for a secure scheme, but by no means a sufficient one. This will be shown in the remaining part of this work.

Section 2 describes the set of (insecure) image encryption algorithms and security "metrics" used in our experimental analysis. In Section 3 results wrt. to security analysis are presented and discussed, while Section 4 presents the conclusions which fundamentally question motivations and security analyses of many chaos-based algorithms for visual data encryption.

2 Encryption Algorithms and Security Assessment Metrics

To foster reproducible research, all software written for this paper, including image encryption techniques, security assessment metrics and the experimental framework, are open source and freely available at GitHub: `https://github.com/mpreis/seth`. Software is implemented in C++. We used the CImg library (`http://cimg.sourceforge.net`) to handle images.

2.1 Encryption Techniques

Baker's map The Baker's map [6] is the probably best known chaotic map. An image is split vertically, stretched horizontally and the resulting pieces are stapled on top of each other. The number of times and the position where the image is split can be chosen arbitrarily and is used as key. This map can be

applied to an image as follows [9]:
Define a sequence $n_1, n_2, \ldots, n_k$ where k is the number of rectangles the image is split into. Each n_i must divide the image width N without remainder and $n_1 + \cdots + n_k = N$. Furthermore, $N_i = n_1 + \cdots + n_i$ and $N_0 = 0$.
Let r with $N_{i-1} \leq r < N_i$ and s with $0 \leq s < N$ a pixel in an $N \times N$ image. Then this pixel $(r,\ s)$ is mapped to: (with $q_i = \frac{N}{n_i}$)

$$B(r,s) = \left(\Big(q_i * (r - N_i) + (s \mod q_i) \Big),\ \Big(\frac{s - (s \mod q_i)}{q_i + N_i} \Big) \right) \tag{1}$$

So far, the algorithm is just a permutation of pixels. To distribute the gray values a substitution is added in the following manner.

Let $(r,\ s)$ be a pixel with gray value g_{rs} which is mapped to $B(r,\ s)$ with gray value $h(r,\ s, g_{rs})$. So, the new gray value depends on the pixel position and the former gray value. A possible way to calculate the new value is the following, where L is the number of gray values:

$$h(r,\ s, g_{rs}) = (g_{rs} + r * s) \mod L \tag{2}$$

Baker's map may be applied several times. The number of iterations used in our experiments is a random number between 10 and 45. To determine the number of slices we generate a set of n random numbers until the sum of these numbers is equal or greater than the width of the image. If the sum is greater than the image width, the last value is replaced by the image width minus the sum of the $n - 1$ previous values. Each number indicates the width of a single slice.

XOR-followers In this approach, deliberately designed to be insecure, a bit is transformed dependent on its following bits. Let k be the length of an arbitrary bitstream key. XOR the next k bits of the current bit with the key and store the resulting bitstream. Then, XOR all bits of this bitstream to get a new bit which is XORed with the current bit. The key space of this algorithm is the worst one considered and the encryption process can also be interpreted as follows. XOR-followers uses the next k bits of an image to calculate the new value of the actual bit. This scheme corresponds to applying a "one-time pad" (OPT) encryption, where the OTP is constructed from the local image content and a fixed key. Obviously, this encryption scheme can not be considered as secure.

We generate a random number which determines the length of the key used for the XOR-followers encryption. There is a minimum length of 8 and a maximum of 256 in our experiments. The next step is to generate a key of length k which is done by taking k random numbers modulo 2.

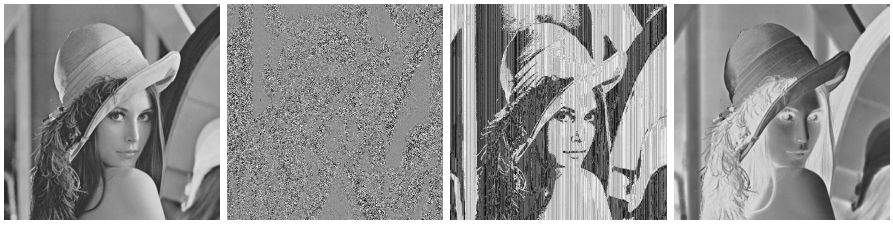
XOR short key is implemented in pixel-mode (encrypts an image pixel by pixel starting at the most significant bit and ends up at the least significant bit)

and MSB-mode (encrypts for every pixel of an image at first the most significant bit (MSB), then for every pixel position MSB-1 and so on).

Instead of creating a one time pad to be used as keystream, this approach simply uses a short key which is XORed repetitively with the image content by shifting the key across the image. In our implementation a short key corresponds to an integer number in its binary representation. An integer number leads to a key space of 2^{32} which is way to small to resist brute-force attacks.

The key is a randomly chosen integer number without any bounds. This scheme is known to be severely insecure, especially on highly redundant data (the most well known attack is termed "counting coincidences" [21]).

Fig. 1 illustrates the encryption of the Lena image with some example configurations. The visual impression of the ciphertexts shown already strongly indicates the almost negligible level of security achieved.



(a) Original (b) XOR-followers (256 bit key) (c) XOR short key pixel (256 bit key) (d) XOR short key MSB (256 bit key)

Fig. 1. Lena image encrypted.

2.2 Security Assessment Metrics

In this section we describe well known security assessment metrics that are used in the majority of papers on chaos-based image and video encryption to experimentally proof the security of their encryption schemes. We have chosen the tests by analysing the experimental section of several papers that propose a chaos-based encryption scheme, see also Table 1.

Correlation property Start with selecting N randomly chosen couples of adjacent pixels from the cipher image. This has to be done three times, for the horizontal, vertical and diagonal correlation property. Then, the correlation coefficient r_{xy} of two adjacent pixels is calculated as follows:

$$\begin{gathered} E(x) = \frac{1}{N} \sum_{i}^{N} x_i, \; D(x) = \frac{1}{N} \sum_{i}^{N} (x_i - E(x))^2 \\ cov(x,y) = \frac{1}{N} \sum_{i}^{N} (x_i - E(x)) * (y_i - E(y)), \; r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} * \sqrt{D(y)}} \end{gathered} \tag{3}$$

x, y are gray values of two adjacent pixels. The correlation coefficient r_{xy} is a value between -1 and 1, where 1 and -1 means highly correlated and 0 uncorrelated. Because neighboring pixels in images are highly correlated, this coefficient should approximate 0 for encrypted images to avoid statistical attacks.

Gray scale histogram uniformity Considering a gray scale histogram of an image one can see a pattern corresponding to the distribution of the relative frequency of the occurring grey values. It is important for an encrypted image to have a different histogram than the original image in particular a uniformly distributed one. We use the variance of the entries of the grey value histogram bins to measure the extent of uniform distribution of an image's histogram. 0 would be a totally uniformly distributed histogram, which would be the optimum for an encrypted image.

NPCR The number of pixel change rate (NPCR) measures the relative number of different pixels in two images I_1 (original) and I_2 (encrypted) and is calculated by the following equation:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{\text{number of pixels}} * 100\% \tag{4}$$

Where

$$D(i,j) = \begin{cases} 0, & I_1(i,j) = I_2(i,j) \\ 1, & \text{otherwise} \end{cases} \tag{5}$$

The higher the better for security, with a maximum of 100%.

UACI Like NPCR, the unified average changing intensity (UACI) is also used to show the difference of two images I_1 (original) and I_2 (encrypted) and is calculated as follows:

$$UACI = \frac{\sum_{i,j} \frac{I_1(i,j) - I_2(i,j)}{\text{tonal range}}}{\text{number of pixels}} * 100\% \tag{6}$$

The result is also in percent, this means the higher the better, with a maximum of 100% but usually values are much lower and highly depend on image content.

3 Experimental evaluation

3.1 Experimental setup

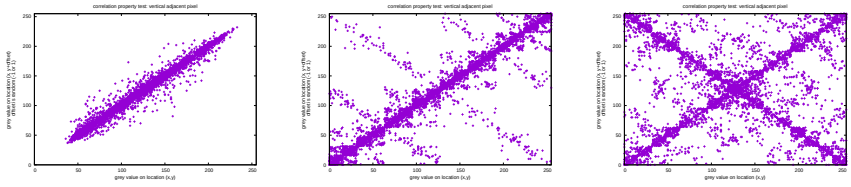
Images & Naming For all our experiments we used the images of the USC-SIPI image database maintained by the University of Southern California and a dataset of standard test images maintained by the University of Granada, overall 128 images. These databases are freely available at `http://sipi.usc.edu/database/` and `http://decsai.ugr.es/cvg/CG/base.htm`. The used images are of size 512 × 512 and 8bpp grey scale. We applied each encryption

technique to each image and executed each test as described in Section 2.2. For each test on every encryption scheme we computed the mean and standard deviation over all images applying 100 randomly selected keys per image. For our visual illustrations we use the famous Lena image which is part of our image pool. In the following section we use shortcuts for the encryption algorithms. Baker's map is denoted *baker*. The substitution-mode of the Baker's map is called *baker-sub*. Further, *xor-key-pix* is used if XOR short key is in pixel-mode and *xor-key-msb* if it is used in MSB-mode. The numbers (*8*, *32* or *256*) at the end of a term indicate the key-length in bit. The XOR followers algorithm is denoted *xor-followers* and again we append the key-length.

3.2 Evaluation results

To provide qualitative results, we use exemplary illustrations of computed values based on the Lena image. Note that this is only meant to visualise basic properties but does not provide any conclusive information, since these visualisations are based on a single image and key only. Quantitative results computed over all images using 100 random keys for each image are provided in tabular form, listing mean values and standard deviation.

Correlation property test In the illustrations, we just focus on the correlation of vertically adjacent pixel pairs. Figure 2.a shows the correlation of the original Lena image. As expected, there is a strong dependency, which is indicated by the clustering of the plotted pixel pairs along a diagonal.



(a) Original Lena (b) XOR short key (pixel mode, 256 bit key) (c) XOR-followers (256 bit key)

Fig. 2. Correlation property (vertical).

Figure 2.b illustrates the correlation of Lena encrypted with the XOR short key algorithm in pixel-mode. As we see there are several areas with a higher concentration of pixel pairs. The most significant concentration is along the diagonal, like in the original Lena image. The pixel pairs are not uniformly distributed. This means there are still dependencies among the pixels. The result for the XOR short key algorithm in MSB-mode is not better.

Figure 2.c shows the correlation of vertical pixel pairs using the XOR-followers algorithm to encrypt the Lena image. The result is slightly better than the result of XOR short key. Nevertheless, most of the pixel pairs can be found along the

diagonals. This shows that there are dependencies between pixel pairs, and this leads to a higher correlation property as also shown by Table 2.

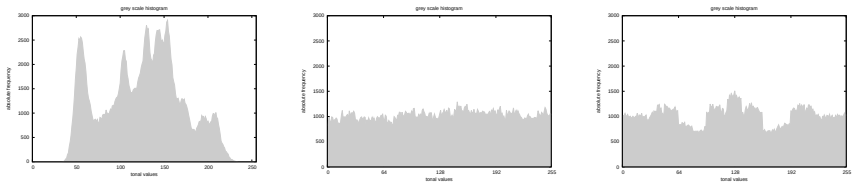
Table 2 shows the quantitative results of the correlation property computed over all images using the considered encryption schemes. Results basically confirm all visual observation made above. Simplistic algorithms like XOR short key or XOR-followers with short key length lead to poor numerical results also supporting the illustrations. The correlation property of XOR-followers with 256 bit key is ≈ 0.04. If we compare this with the result of the Baker's map, which is 0.002984, we see a large difference. In terms of correlation, chaos-based schemes lead to superior results compared to the deliberately insecure schemes.

Table 2. Average correlation properties over all tested images.

Encryption	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
	Mean			(Standard deviation)		
xor-key-pix-8	0.710550	0.387219	0.347165	(0.021387)	(0.060259)	(0.054845)
xor-key-pix-32	0.715003	0.397949	0.356478	(0.018945)	(0.039519)	(0.037896)
xor-key-pix-256	0.714619	0.399354	0.357709	(0.018529)	(0.034743)	(0.03362)
xor-key-msb-8	0.886602	0.874574	0.809875	(0.008905)	(0.011872)	(0.023852)
xor-key-msb-32	0.886792	0.874621	0.810086	(0.008856)	(0.011891)	(0.02381)
xor-key-msb-256	0.886764	0.874547	0.810003	(0.008872)	(0.011905)	(0.023846)
xor-followers-8	0.146756	0.146240	0.124010	(0.0374)	(0.038542)	(0.031647)
xor-followers-32	0.073218	0.088525	0.055907	(0.032644)	(0.026302)	(0.023301)
xor-followers-256	0.049615	0.060557	0.033824	(0.025877)	(0.01439)	(0.012841)
baker-sub	0.003207	0.000050	0.000018	(0.001295)	(0.000208)	(0.000202)
baker	0.002984	0.000100	0.000072	(0.00132)	(0.000276)	(0.000262)

Contrasting to other metrics, standard deviation is not larger for worse encryption schemes (see e.g. rather low standard deviation for XOR short key algorithms even for short key length).

Grey scale histogram Figure 3 shows the grey scale histogram of the original Lena image. As expected the grey scale values are not uniformly distributed in the original. As shown in the figure there are several spikes and there are values which are not attained in the original image.



(a) Original Lena (b) XOR short key (pixel-mode, 256 bit key) (c) XOR-followers (256 bit key)

Fig. 3. Grey scale histograms.

The XOR short key algorithm influences the grey scale values and changes their distribution in the histogram. Therefore, the values are much better distributed than in the original image, which is shown in Figure 3.b. However, we are far from achieving a perfectly flat histogram.

The grey scale histogram of the XOR-followers algorithm shows uniform distribution of the grey scale values only to a medium extent. If we take a closer look we see that there are several spikes which seam to occur periodically, see Figure 3.c. Again, the distribution is not as smooth as would be expected from a perfect algorithm.

Table 3 shows the corresponding quantitative results, i.e. average variance of the grey scale histogram bins over all images. A small value indicates that the gray scale values of an image are uniformly distributed. This test confirms the qualitative results of the displayed grey scale histograms and reports excellent values for Baker's map in substitution mode only. However, the deliberately insecure schemes are still clearly superior to the "pure" chaotic scheme without substitution (both in terms of mean and standard deviation). There is a mix of XOR-followers and XOR short key in pixel mode found as group of second best techniques, where longer keys do not necessarily provide better results.

Table 3. Grey-scale histogram bin variance.

Encryption	Mean variance	Standard deviation
xor-key-pix-8	5745.642493	6787449468.58157
xor-key-pix-32	5393.119154	15956913550.987
xor-key-pix-256	2075.310975	19580730.204758
xor-key-msb-8	1029635.438768	173086477183998
xor-key-msb-32	1159182.716775	203421440346693
xor-key-msb-256	1100090.429456	189863134653252
xor-followers-8	2924.137718	212041579.480851
xor-followers-32	23195.459391	2735952915334.39
xor-followers-256	21408.063662	3244132007115.65
baker-sub	6.330361	238.709062
baker	2086390.600900	351119352268353

So far, we have observed inconsistencies wrt. algorithm ranking concerning different metrics: While for the correlation values, both chaos-based encryption schemes deliver better values compared to the deliberately insecure variants, for the histogram-bin variance only Baker's map in substitution mode is better than those algorithms. The permutation-only chaotic scheme is the worst one. Also, the ranking among XOR-followers and the variants of XOR short key is not consistent among the two metrics discussed so far.

NPCR and UACI NPCR values have their theoretical maximum at 100% while for UACI there is no theoretical maximum, however it is evident that higher values are better. Taking a look at Table 4 we see that the NPCR values of XOR short key in MSB-mode are the worst ones. All other values are above 99%, except for the permutation only chaos-based scheme, the best mean value

is attained by the XOR-followers with 32 bit key (only the standard deviation is larger compared to Baker's map with substitution). When comparing the computed values with our illustrative encrypted image examples, we note that in the example of the XOR-followers image there are some parts which likely correspond to contours – even though, this approach leads to a very good NPCR value. If we compare the visual encryption result and the NPCR value of the XOR short key algorithm we notice that Lena is still recognisable in both variants. In MSB-mode, as expected, we get a bad NPCR result, but the pixel-mode reaches a value over 99 percent. The NPCR value of XOR short key and XOR-followers algorithms turns out to be independent of the key length.

Table 4 presents the results the UACI test as well. Algorithms with good results in the NPCR test, also exhibit good results result in the UACI test, however, UACI seems to be more discriminative. Baker's map stays under 20 percent, which is one of the worst results. Interestingly, XOR followers with a 32 bit key again performs best with an UACI of 32.9. The XOR short key algorithm in pixel mode gives very poor values. That is remarkable, because this XOR short key variant has an NPCR value over 99 percent. The results show, that the key-length does not lead to better result for XOR short key and XOR followers. We conclude that most of the NPCR test results are confirmed by the UACI test. Encryption schemes with a solid NPCR result also pass at the UACI test, except for XOR short key.

Table 4. Average UACI and NPCR test results.

Encryption	UACI	NPCR	UACI	NPCR
	Mean		(Standard deviation)	
xor-key-pix-8	16.521567	99.241211	(18.667307)	(43.775804)
xor-key-pix-32	16.102003	99.089111	(6.047226)	(7.907319)
xor-key-pix-256	16.122123	99.036255	(2.554497)	(1.115388)
xor-key-msb-8	22.266539	49.492188	(620.447027)	(2499.937434)
xor-key-msb-32	22.337422	49.960938	(613.269976)	(2500.193802)
xosr-key-msb-256	22.544910	50.289062	(617.188992)	(2500.111764)
xor-followers-8	27.916054	99.519661	(65.655065)	(0.062579)
xor-followers-32	32.908797	99.652940	(32.978066)	(2.081644)
xor-followers-256	30.150691	99.455602	(59.791081)	(0.861717)
baker-sub	31.948774	99.608591	(14.196343)	(0.000165)
baker	19.527519	97.055924	(70.996208)	(53.389462)

Summarising, NPCR and UACI exhibit further weaknesses: XOR-followers with 32 bit key, an obviously weak encryption scheme, results in the best values. Second, the chaos-based scheme with permutation-only is only better as XOR short key schemes in pixel mode (UACI) or MSB mode (NPCR). UACI is the only metric which does not rate XOR short key in MSB mode as the worst algorithm group. And third, maybe worst, NPCR does not clearly detect (values still beyond 99%) encryption schemes clearly exhibiting visual defects. An additional issue with UACI is that even well performing technique exhibit very

large standard deviation, indicating a significant dependence on image nature and structure.

4 Conclusion

We have identified and discussed three weaknesses in security-related issues wrt. chaos-based image and video encryption. First, we demonstrate that a commonly used motivation to employ these encryption primitives instead of classical, cryptographically strong ciphers is not valid as modern encryption primitives – for which the IND-CPA assumption is supposed to be valid – do not exhibit the claimed weaknesses when it comes to encrypting highly redundant and correlated data (like image data). Second, an obvious weakness is the high number of broken chaos-based image and video encryption schemes. More severe, typically this fact is ignored in manuscripts proposing new schemes in which of course it should be made clear in how far a new cipher is able to withstand all the demonstrated attacks against related schemes. Third, we were able to experimentally demonstrate that deliberately chosen low-security encryption schemes do not clearly fail a battery of tests for experimental security evaluation, which are commonly used to assess chaos-based encryption schemes for visual data. In particular, we have noticed that

- for NPCR and UACI, XOR-followers with 32 bit key (almost ridiculously low security) is ranked superior to all chaos-based encryption variants;
- for most security "metrics" deliberately weak schemes are rated superior to the permutation-only chaos-based cipher;
- the ranking among the considered encryption algorithms and their variants based on the metrics' values is not at all consistent and thus does not seem to allow any implication about the level of security achieved;
- even visually obvious security deficits are not detected by all metrics considered;
- a very high standard deviation can be observed for many metrics (in many cases associated with low quality mean) emphasising the importance of using large scale image sets and key spaces in experimentation.

Therefore, the commonly used way to experimentally assess security of these schemes is severely questioned since it has to be clear that even passing these tests is necessary for security, but is by no means a sufficient criterion (as spectacularly demonstrated by the multitude of broken algorithms passing these tests).

References

[1] Ahmad, M., Imran, R., Shazhad, A.: Cryptanalysis of image encryption algorithm based on fractional-order lorenz-like chaotic system. In: Emerging ICT for Bridging the Future (Vol. 2), Advances in Intelligent Systems and Computing, vol. 338, pp. 381–388. Springer (2015)

[2] Ahmad, M.: Cryptanalysis of chaos based secure satellite imagery cryptosystem. In: Contemporary Computing, Communications in Computer and Information Science, vol. 168, pp. 81–91. Springer (2011)

[3] Alvarez, E., Fernandez, A., Garcıa, P., Jiménez, J., Marcano, A.: New approach to chaotic encryption. Physics Letters A 263(4), 373–375 (1999)

[4] Alvarez, E., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of a chaotic encryption system. Physics Letters A 276(4), 191–196 (2000)
[5] Alvarez, G., Amigó, J.M., Arroyo, D., Li, S.: Chaos-Based Cryptography: Theory,Algorithms and Applications, chap. Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers, pp. 257–295. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
[6] Balatoni, J., Renji, A.: On the notion of entropy (Hungarian). Publ. Math. Inst. Hungarian Acad. Sci. 1(9), 9–40 (1956)
[7] Chen, R., Lu, W., Lai, J.: Image encryption using progressive cellular automata substitution and SCAN. In: Proceeding of IEEE International Symposium on Circuits and Systems (vol. 2). pp. 1690–1693 (2005)
[8] Cokal, C., Solak, E.: Cryptanalysis of a chaos-based image encryption algorithm. Physics Letters A 373, 1357–1360 (2009)
[9] Fridrich, J.: Image encryption based on chaotic maps. In: Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on. vol. 2, pp. 1105–1110. IEEE (1997)
[10] Gao, T., Chen, Z.: A new image encryption algorithm based on hyper-chaos. Physics Letters A 372(4), 394–400 (2008)
[11] Guan, Z.H., Huang, F., Guan, W.: Chaos-based image encryption algorithm. Physics Letters A 346(1), 153–157 (2005)
[12] Hussain, I., Shah, T., Gondal, M.A.: Image encryption algorithm based on total shuffling scheme and chaotic s-box transformation. Journal of Vibration and Control 20(14), 2133–2136 (2014)
[13] Jeng, F.G., Huang, W.L., Chen, T.H.: Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes. Signal Processing: Image Communication 34, 45–51 (2015)
[14] Li, C., Lo, K.T.: Cryptanalysis of an image encryption scheme using cellular automata substitution and SCAN. In: Advances in Multimedia Information Processing (Proceedings of PCM 2010). pp. 601–610. Springer (2010)
[15] Li, S., Mou, X., Cai, Y.: Improving security of a chaotic encryption approach. Physics Letters A 290(3-4), 127–133 (2001)
[16] Lian, S., Sun, J., Wang, Z.: Security analysis of a chaos-based image encryption algorithm. Physica A: Statistical Mechanics and its Applications 351(2), 645–661 (2005)
[17] Menezes, A.J., Vanstone, S.A., van Oorschot, P.C.: Handbook of Applied Cryptography (5th printing). CRC Press (2001)
[18] Mishra, M., Mankar, V.: Review on chaotic sequences based cryptography and cryptanalysis. International Journal of Electronics Engineering 3(2), 189–194 (2011)
[19] Rhouma, R., Belghith, S.: Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Physics Letters A 372(38), 5973–5978 (2008)
[20] Scharinger, J., Pichler, F.: Efficient image encryption based on chaotic maps. In: Proceedings of the 20th Workshop of the Austrian Association for Pattern Recognition (OAGM/AAPR'96) on Pattern Recognition. pp. 159–170. Oldenbourg Verlag, Munich, Germany (1996)
[21] Schneier, B.: Applied cryptography (2nd edition): protocols, algorithms and source code in C. Wiley Publishers (1996)
[22] Sharma, P., Ahmad, M., Khan, P.: Cryptanalysis of image encryption algorithm based on pixel shuffling and chaotic S-box transformation. In: Security in Computing and Communication, Communications in Computer and Information Science, vol. 467, pp. 173–181. Springer (2014)
[23] Solak, E., Cokal, C., Yildiz, O., Biyikoglu, T.: Cryptanalysis of fridrich's chaotic image encryption. International Journal on Bifurcation and Chaos 20(5), 1405–1413 (2010)
[24] Solak, E.: Chaos-Based Cryptography: Theory,Algorithms and Applications, chap. Cryptanalysis of Chaotic Ciphers, pp. 227–256. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
[25] Usama, M., Khan, M., Alghathbar, K., Lee, C.: Chaos-based secure satellite imagery cryptosystem. Computers and Mathematics with Applications 60(2), 326–337 (2010)
[26] Wang, X., Teng, L., Qi, X.: A novel colour image encryption algorithm based on chaos. Signal Processing 92(4), 1101–1108 (2012)
[27] Wang, X., Guo, K.: A new image alternate encryption algorithm based on chaotic map. Nonlinear Dynamics 76(4), 1943–1950 (2014)
[28] Wu, Y., Noonan, J., Again, S.: NPCR and UACI randomness tests for image encryption. Cyber Journals: Journal of Selected Areas in Telecommunications (JSAT) 4, 31–38 (2011)
[29] Xu, Y., Wang, H., Li, Y., Pei, B.: Image encryption based on synchronization of fractional chaotic systems. Communications in Nonlinear Science and Numerical Simulation 19(10), 3735–3744 (2014)
[30] Yap, W.S., Phan, R.C.W., Yau, W.C., Heng, S.H.: Cryptanalysis of a new image alternate encryption algorithm based on chaotic map. Nonlinear Dynamics 80(3), 1483–1491 (2015)
[31] Ye, G.D.: Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recognition Letters 31, 347–354 (2010)
[32] Yen, J.C., Chen, H.C., Wu, S.M.: Design and implementation of a new cryptographic system for multimedia transmission. In: Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on. pp. 6126–6129. IEEE (2005)
[33] Zhao, L., Adhikari, A., Xiao, D., Sakurai, K.: Cryptanalysis on an image scrambling encrytion scheme based on pixel bit. In: Digital Watermarking: 9th International Workshop, IWDW 2010, Lecture Notes on Computer Science (LNCS), vol. 6526, pp. 45–59. Springer (2010)