Plaintext type	Characteristics	Implications for stegotext
New non-EB-like	• Security and automatability dependent on stegotext type	• If stegotext is different new non-EB-like information, automatable in theory, secure against **Type I** adversaries but **not** perfectly secure since Type II adversary can detect mere instantiation of steganography consciously (e.g., if all other Type II entities stop to send any message that is *not* a new EB). • If stegotext is old EB, automatable in theory but **neither** efficient in practice (due to hard string-level mapping to old EBs which are harder-to-vary than any old non-EB-like information) **nor** perfectly secure since Type I adversary could automatically detect mere instantiation of steganography and Type II adversary could detect it consciously. • If stegotext is new EB, **neither** automatable **nor** efficient in practice (due to hard string-level mapping to new EBs which are harder-to-vary than any other information). • If stegotext=plaintext, it is efficient and automatable but **minimally secure** since it is not only the case that Type II adversary could detect mere instantiation of steganography consciously, but obviously the plaintext would directly be available too.
Old EBs or old non-EB-like information	• Not informative, extremely limited utility • Security and automatability dependent on stegotext type	• If stegotext is old non-EB-like information different from plaintext, automatable in theory but **not** perfectly secure in practice since Type I adversary could automatically detect instantiation of steganography and Type II adversary could detect it consciously. • If stegotext is new non-EB-like information, automatable in theory, secure against **Type I** adversaries but **not** perfectly secure since Type II adversary can detect mere instantiation of steganography consciously (e.g., if all other Type II entities stop to send any message that is *not* a new EB). • If stegotext is old EB different from plaintext, automatable in theory but **neither** efficient in practice (due to hard string-level mapping to old EBs which are harder-to-vary than any old non-EB-like information) **nor** perfectly secure since Type I adversary could automatically detect instantiation of steganography and Type II adversary could detect it consciously. • If stegotext is new EB, **neither** automatable **nor** efficient in practice (due to hard string-level mapping to new EBs which are harder-to-vary than any other information).

		• If stegotext=plaintext, it is efficient and automatable but **minimally secure** since it is not only the case that Type I adversary could automatically detect mere instantiation of steganography and Type II adversary could detect it consciously, but obviously the plaintext would directly be available too.
New EBs	• Impossibility of automatibility irrespective of stegotext type	• If stegotext is non-EB-like, **neither** automatable **nor** perfectly secure in practice since Type II adversary can detect mere instantiation of steganography consciously (e.g., if all other Type II entities stop to send any message that is *not* a new EB). • If stegotext is old EB, **neither** automatable, **neither** efficient in practice (due to hard string-level mapping to old EBs which are harder-to-vary than any old non-EB-like information) **nor** perfectly secure since Type I adversary could automatically detect mere instantiation of steganography and Type II adversary could detect it consciously. • If stegotext is <u>different</u> new EB, **neither** automatable **nor** efficient *at first sight* (due to hard string-level mapping to new EBs which are harder-to-vary than any other information), however the plaintext **is** perfectly secure from **Type I** adversaries; if stegotext is higher-level EB than plaintext, the stegotext implies the plaintext such that Type II adversary could only *inherently* retrieve plaintext if and only if plaintext is already understood even if stegotext is <u>not</u> yet understood (interestingly, if stegotext is *not* directly understood by Type II adversary, stegotext will appear like new *non*-EB-like information, but even in this case mere instantiation of steganography will still be detected); if stegotext is lower-level EB than plaintext, the plaintext implies the stegotext such that Type II adversary could <u>not</u> inherently retrieve plaintext if stegotext is not yet understood (even if stegotext is *not* directly understood by Type II adversary, stegotext will appear like new *non*-EB-like information, in this case mere instantiation of steganography will still be detected). • If stegotext=plaintext, **neither** automatable **nor** efficient in practice (due to hard string-level mapping to new EBs which are harder-to-vary than any other information), however the plaintext **is** perfectly secure from **Type I** adversaries; Type II adversary *inherently*

		retrieves plaintext if and only if stegotext is understood. For Type II adversaries, it is possible to reveal any communication via non-EB-like information or old EBs as potential attempt of automatable steganography. The Type II defense consists in imposing communication via new EBs only which is safe from Type I adversaries. However, Type II entities can still always suspect new EB messages to potentially be a non-automatable highly inefficient steganography attempt to communicate old EBs, new or old non-EB-like information. Moreover, a Type II adversary could also suspect a just perceived new EB message (i.e. the potential stegotext) to be hiding *higher-level* new EB plaintexts (which is what is lucrative in the context of intellectual property for instance). Naturally, it could also be hiding a lower-level new EB plaintext. But that would not be logical to hide the latter from an adversary that could understand an even more valuable sensitive information in the stegotext. So, one could state that **hiding higher-level new EBs in lower-level new EBs** is more efficient than hiding lower-level new EBs in higher-level new EBs. In short, certain "inefficiently" appearing high-energetic processes may actually be efficient e.g., *if being highly important but occurring comparatively speaking extremely rarely*. The epistopological Type II adversary is aware of all that. For this reason, steganography, which attempts to hide the mere presence of any covertext at all, does not exist for an epistopological adversary[1]. Instead, the dynamics of the entire universe seem to become a gamified process of *epistopological cryptography* based on new EBs and what they may hide ad infinitum. This may be related to the miraculous *comprehensibility* underlying the eternal mystery of the universe as perceived by Einstein. The secret is that new EBs could hide *all* there could be.

[1] There are fears that Type I AI could use encoded reasoning to hide information that no human could understand. In light of the above, it becomes clear that for a Type II adversary, the world stays comprehensible with the described epistopological cryptographic strategies. Note that an EB-based encoded reasoning (i.e., based on a plaintext meta-blockchain of successive better and better new EBs where some steps in between would be omitted) is not only **impossible** for a Type I entity due to the impossibility to automate new EB generation, but also, it is even impossible for a Type **II** entity. The latter holds because one cannot skip a step in the process of creating successive better new EBs (see also cynet bulk dynamics) – by what a Type II adversary would be able to sense a disruption of a meta-EB-blockchain. For illustration purposes, consider a new EB from cynet bulk layer 3 presented directly after a new EB from cynet bulk layer 1. Either the Type II adversary already knows that something is missing, or the new EB from layer 3 is not yet understood and then labelled as new non-EB-like material – which means the meta-EB-blockchain is broken in any case and the attempt of EB-based encoded reasoning resulted in a failure.